FINITE p-IRREGULAR SUBGROUPS OF $\mathrm{PGL}_2(k)$

XANDER FABER

Abstract. Following Beauville in the p-regular case, we give a classification of the finite p-irregular subgroups of $\mathrm{PGL}_2(k)$, up to conjugation, for an arbitrary field k of positive characteristic p. For algebraically closed fields, the proof follows the strategy of Dickson for classifying subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$. The general case follows by Galois descent.

1. Introduction

The finite subgroups of rotations of the round 2-sphere have been understood at least since the work of Klein [5]. In modern parlance, we could say that Klein understood the classification of finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$, the group of invertible complex matrices modulo scalar matrices. Around the same time that Klein was writing his book on the icosahedron, Dickson was reading the papers of Galois, Jordan, and others with the intent to classify subgroups of linear groups in characteristic p such as $\mathrm{PSL}_2(\mathbb{F}_q)$ — the group of invertible matrices with $\mathbb{F}_q$-coefficients and determinant 1 modulo scalar matrices [3].

Recently Beauville gave a beautiful, modern exposition of the classification of finite subgroups of $\mathrm{PGL}_2(k)$ of order prime to $\mathrm{char}(k)$ — for an arbitrary field k — using Galois cohomology [1]. His proof takes advantage of the accidental isomorphism $\mathrm{PGL}_2(k) \cong \mathrm{SO}(k,q)$, where the latter is the special orthogonal group for the quadratic form $q(x,y,z) = x^2 + yz$. (This isomorphism exists because $\mathrm{PGL}_2(k)$ is the automorphism group of the projective line, which may be embedded in $\mathbb{P}^2$ as the conic $x^2 + yz = 0$.) In the present paper, we extend this classification to *arbitrary* finite subgroups $G \subset \mathrm{PGL}_2(k)$. The case of new interest is then an infinite field of characteristic $p > 0$ and a subgroup G whose order is divisible by p — a p-irregular subgroup. We learn that a finite p-irregular subgroup of $\mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for q a power of the characteristic of k, to a p-semi-elementary group (see the next section for the definition), to a dihedral group, or to $\mathfrak{A}_5$. Theorem A gives the conditions for existence of these types of subgroups, and Theorem B gives the classification up to conjugacy inside $\mathrm{PGL}_2(k)$.

The subgroups of PGL_2 came into the author's spotlight as automorphism groups of discrete dynamical systems on the projective line [7, Ch. 4.8]. Given a rational function $\phi \in \mathbb{Q}(z)$, the automorphism group is $\mathrm{Aut}_\phi(\mathbb{Q}) = \{f \in \mathrm{PGL}_2(\mathbb{Q}) : f \circ \phi \circ f^{-1} = \phi\}$. In a subsequent paper [4], the author, Manes, and Viray design an algorithm for computing $\mathrm{Aut}_\phi(\mathbb{Q})$ by piecing it together from $\mathrm{Aut}_\phi(\mathbb{F}_p) \subset \mathrm{PGL}_2(\mathbb{F}_p)$ for several primes p of good reduction for ϕ; evidently the classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ up to conjugation is invaluable for such a pursuit. Such a classification does not seem to appear explicitly in the literature, and so we deduce it as a special case of the main results of the present paper. See Theorem D in the next section. (We note that Dickson [3, §260] does give a classification for subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$, from which Theorem D can be deduced with a small amount of work.)

This paper has two main parts, which are somewhat disparate in nature. The first part — Sections 3 through 6 — is devoted to following Dickson's arguments in [3, §239–261] in order to

Date: March 15, 2012.

The author would like to acknowledge the partial support of the NSF through its Postdoctoral Fellowship program, and he would like to thank Geoff Robinson (via MathOverflow) for pointing him to Dickson's work on the subject.

give a complete classification of finite subgroups of $\mathrm{PGL}_2(k)$ when k is algebraically closed. (This seems to be the same argument used by Klein.) Dickson's proof is very elementary — it uses only some basics of group actions, the Sylow theorems, and a little knowledge of the action of $\mathrm{PGL}_2(k)$ on $\mathbb{P}^1(k)$. We have endeavored to keep this part of the paper completely elementary and as self-contained as possible; it could serve as the basis for a reading project by an undergraduate with a background in abstract algebra. As a natural byproduct of this approach, we were able to recover the classical description of finite p-regular subgroups of $\mathrm{PGL}_2(k)$ for an algebraically closed field k (cf. Theorem C). We note that a list of isomorphism types of subgroups of $\mathrm{PSL}_2(k)$ for k algebraically closed appears in Suzuki's book [8, Thm. 6.17], but no classification of conjugacy classes is given.

The second part of this paper — Sections 7 and 8 — completes the classification of finite subgroups of $\mathrm{PGL}_2(k)$ by first passing to separably closed fields, and then by applying Galois descent. This part is less elementary and draws heavily from Beauville's paper [1]. The main idea is to use a cohomological parameterization of the distinct conjugacy classes of subgroups in $\mathrm{PGL}_2(k)$ that coincide over a separable closure of k. For p-irregular subgroups, the relevant cohomology set turns out to be trivial, and so we reduce to the case of separably closed fields. In this sense, the classification of p-irregular subgroups is *easier* than its p-regular counterpart.

We close this section with a more precise description of the contents of the article. The next section contains our notational conventions and the statements of the main theorems. Section 3 collects a number of invaluable trace/determinant equations that characterize when an element of $\mathrm{PGL}_2(k)$ has a certain small order. In Section 4, we study several seemingly special subgroups of $\mathrm{PGL}_2(k)$; we then show that these special cases exhaust all possible finite subgroups in Sections 5 (p-regular subgroups) and 6 (p-irregular subgroups). We will restrict to the case in which k is algebraically closed in Sections 3 through 6. Ignoring the question of when certain equations actually have solutions in k clarifies the presentation dramatically, and so we were able to make this portion of the paper completely elementary. In Section 7 we pass to separably closed fields k; this requires extra work only in characteristic 2. Section 8 contains the Galois cohomology computation necessary to pass from separably closed fields to the general case, and it contains the proofs of the main theorems.

2. The Classification

In this article, we write $\mathrm{PGL}_2(k) = \mathrm{GL}_2(k)/k^\times$, and elements of $\mathrm{PGL}_2(k)$ will be represented by (equivalence classes of) matrices $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ with $\alpha\delta - \beta\gamma \neq 0$. Here $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) = \left(\begin{smallmatrix}\lambda\alpha & \lambda\beta\\ \lambda\gamma & \lambda\delta\end{smallmatrix}\right)$ for any $\lambda \neq 0$. We write I for the identity of $\mathrm{PGL}_2(k)$. An element $s \in \mathrm{PGL}_2(k)$ acts on $\mathbb{P}^1(k) = k \cup \{\infty\}$ by the formula $s.z = \frac{\alpha z+\beta}{\gamma z+\delta}$.

The letter q will always denote a power of p. We say that an element of a finite group G is p-regular if its order is prime to p, and we say that G is p-regular if all of its elements are p-regular. Otherwise, an element or a group is p-irregular.

For the following statements, we will use the notation $\mathfrak{D}_n$, $\mathfrak{S}_n$, and $\mathfrak{A}_n$ for the dihedral group with $2n$ elements, the symmetric group on n letters, and the alternating group on n letters, respectively. An abstract finite group G will be called **p-semi-elementary** if it has a unique Sylow p-subgroup P of exponent p with G/P cyclic. Write $\mu_n(k)$ for the group of n-th roots of unity in k.

For any field k, the determinant map $\det : \mathrm{GL}_2(k) \to k^\times$ descends to a homomorphism $\overline{\det} : \mathrm{PGL}_2(k) \to k^\times/(k^\times)^2$. Write $\mathrm{PSL}_2(k)$ for the kernel of $\overline{\det}$.

As we will see in Theorem B, any finite p-irregular subgroup of $\mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some q, to a p-semi-elementary group, to a dihedral group, or to $\mathfrak{A}_5$. The following theorem describes the precise conditions under which these types of subgroups exist in $\mathrm{PGL}_2(k)$.

Theorem A (Existence of Finite p-Irregular Subgroups)**.** Let k be a field of characteristic $p > 0$.

(1) Let q be a power of p. Then $\mathrm{PGL}_2(k)$ contains subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q)$ if and only if $\mathbb{F}_q \subset k$.
(2) Let $m \in \mathbb{N}$ and $n \in \mathbb{N} \smallsetminus p\mathbb{N}$, and let e be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathrm{PGL}_2(k)$ contains p-semi-elementary subgroups of order $p^m n$ if and only if $\mathbb{F}_{p^e} \subset k$ and $e \mid m \leq \dim_{\mathbb{F}_p}(k)$.[1]
(3) If $p = 2$ and $n \in \mathbb{N}$ is odd, then $\mathrm{PGL}_2(k)$ contains dihedral subgroups $\mathfrak{D}_n$ if and only if $\zeta + \zeta^{-1} \in k$ for some primitive n-th root of unity ζ.
(4) If $p = 3$, then $\mathrm{PGL}_2(k)$ contains subgroups isomorphic to $\mathfrak{A}_5$ if and only if $\mathbb{F}_9 \subset k$.

Theorem B (Classification of Finite p-irregular subgroups)**.** Let k be a field of characteristic $p > 0$. Any finite p-irregular subgroup of $\mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some q, to a p-semi-elementary group, to a dihedral group, or to $\mathfrak{A}_5$.

(1) Fix q a power of p such that $\mathbb{F}_q \subset k$. There is exactly one conjugacy class of subgroups isomorphic to each of $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$.
(2) Let $n \in \mathbb{N} \smallsetminus p\mathbb{N}$ and $m \in \mathbb{N}$ with $p^m n > 2$. Write e for the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. The conjugacy classes of p-semi-elementary subgroups of order $p^m n$ are parameterized by the set of homothety classes[2] of rank-m subgroups Γ satisfying $\mathbb{F}_{p^e} \subset \Gamma \subset k$ via the map
$$\Gamma \mapsto \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix}.$$
(3) Suppose that $p = 2$ and n is an odd positive integer such that $\lambda := \zeta + \zeta^{-1} \in k$ for some primitive n-th root of unity ζ. Let $\mathfrak{Dih}_n(k)$ denote the set of conjugacy classes of dihedral subgroups of $\mathrm{PGL}_2(k)$ of order $2n$. The map $\mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ defined by $G \mapsto \overline{\det}(t)$ for any involution $t \in G$ is well defined and injective. This map is surjective if $n = 1$, and otherwise its image in $k^\times/(k^\times)^2$ is the set of nonzero elements represented by the quadratic form $x^2 + \lambda xy + y^2$.
(4) If $\mathbb{F}_9 \subset k$, then there is exactly one conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.

Any p-irregular subgroup of $\mathrm{PGL}_2(k)$ is among the four types listed here.

Remark 2.1. It is worth noting that dihedral and p-semi-elementary subgroups may be characterized geometrically as follows. A subgroup of $\mathrm{PGL}_2(k)$ (p-regular or not) is dihedral if and only if it stabilizes a pair of distinct points of $\mathbb{P}^1(k)$, but does not fix them. A subgroup is p-semi-elementary if it fixes a unique point of $\mathbb{P}^1(k)$.

The methods used to prove Theorem B allow us, with essentially no extra work, to give an elementary classification of the finite p-regular subgroups of $\mathrm{PGL}_2(k)$ up to conjugation when k is separably closed. By elementary, we mean that it avoids the use of representation theory; see [1] for the representation theory approach and for analogues of Theorems A and B for p-regular finite subgroups.

Theorem C (Finite p-regular subgroups)**.** Let k be a separably closed field, and let G be a finite subgroup of $\mathrm{PGL}_2(k)$ such that $p \nmid |G|$. Then up to conjugation, G is one of the following subgroups:

(1) $G = \left\langle \left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right) \right\rangle$ for some $\zeta \in k^\times$; here G is cyclic.
(2) $G = \left\langle \left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right) \right\rangle \rtimes \left\langle \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) \right\rangle$ for some $\zeta \in k^\times$; here G is dihedral.
(3) $G = N \rtimes C \cong \mathfrak{A}_4$, where $N = \left\{ \left(\begin{smallmatrix} \pm 1 & \\ & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \\ & \pm 1 \end{smallmatrix}\right) \right\}$ and $C = \left\{ I, \begin{pmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -\sqrt{-1} & \sqrt{-1} \end{pmatrix} \right\}$.
(4) $G = \left\langle T, \left(\begin{smallmatrix} \sqrt{-1} & \\ & 1 \end{smallmatrix}\right) \right\rangle \cong \mathfrak{S}_4$, where $T = N \rtimes C \cong \mathfrak{A}_4$ is the group in (3).

[1] The condition $\mathbb{F}_{p^e} \subset k$ is equivalent to the assertion that there is a primitive n-th root of unity in k.
[2] Two subgroups $\Gamma, \Gamma' \subset k$ are **homothetic** if $\Gamma' = \alpha\Gamma$ for some $\alpha \in k^\times$.

(5) $G = \langle s, t\rangle \cong \mathfrak{A}_5$, where $s = \left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$, $t = \left(\begin{smallmatrix} 1 & 1-\lambda-\lambda^{-1} \\ 1 & -1 \end{smallmatrix}\right)$, and λ is any primitive fifth root of unity in $k^\times$. These generators satisfy $s^5 = t^2 = (st)^3 = I$.

In particular, if $G, G' \subset \mathrm{PGL}_2(k)$ are (abstractly) isomorphic finite groups, then they are conjugate.

Finally, as a concrete application of these results we characterize all subgroups of the projective linear group over a finite field.

Theorem D. Let $\mathbb{F}_q$ be a finite field with $q = p^r$, and write $G = \mathrm{PGL}_2(\mathbb{F}_q)$. Each subgroup of G is described by one of the following cases:

(1) If $q \equiv \pm 1 \pmod{n}$, then G contains a unique conjugacy class of cyclic subgroups of order n and of dihedral subgroups of order $2n$.
(2) If p is odd, or if $p = 2$ and r is even, then G contains a unique conjugacy class of subgroups isomorphic to $\mathfrak{A}_4$.
(3) If $p \neq 2$, then G contains a unique conjugacy class of subgroups isomorphic to $\mathfrak{S}_4$.
(4) If $p \equiv 0, \pm 1 \pmod 5$, or if $p \equiv \pm 2 \pmod 5$ and r is even, then G contains a unique conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.
(5) If $s \mid r$, then G contains a unique conjugacy class of subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{p^s})$ and $\mathrm{PSL}_2(\mathbb{F}_{p^s})$.
(6) If $m \in \mathbb{N}_{\leq r}$, $n \in \mathbb{N} \smallsetminus p\mathbb{N}$, and $e \mid (r, m)$, where e is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, then G contains p-semi-elementary subgroups of order $p^m n$. The conjugacy classes of such subgroups are in bijection with the set of homothety classes of rank-m subgroups of $\mathbb{F}_q$ containing $\mathbb{F}_{p^e}$.

3. Fixed points

Convention. Throughout this section we will assume k is an algebraically closed field.

The interplay between $\mathrm{PGL}_2(k)$ as a matrix group and its action on $\mathbb{P}^1(k)$ is often realized through the following two observations. Write $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Then $s.\infty = \alpha/\gamma$, so that α/γ is a meaningful invariant of the (equivalence class of) s. If $s.z$ fixes the point $x \in \mathbb{P}^1(k)$, and if $t \in \mathrm{PGL}_2(k)$ satisfies $t.x = y$, then $(tst^{-1}).z$ fixes y. In this case, we say that we have conjugated the fixed point of s to y.

If $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ is a nontrivial element of finite order, then s has either one or two distinct fixed points in $\mathbb{P}^1(k)$ given by the equation

$$\gamma z^2 + (\delta - \alpha)z - \beta = 0. \tag{3.1}$$

If s has a unique fixed point, we may conjugate it to ∞ to see that $s.z = z + \beta$, or in matrix form: $s = \left(\begin{smallmatrix} 1 & \beta \\ & 1 \end{smallmatrix}\right)$. Since $s^m = \left(\begin{smallmatrix} 1 & m\beta \\ & 1 \end{smallmatrix}\right)$, we find s has order $p = \mathrm{char}(k) > 0$.

Conversely, if $s \in \mathrm{PGL}_2(k)$ has order $p > 0$, then we claim that s has a unique fixed point. For suppose s has two distinct fixed points, and let us conjugate them to 0 and ∞. Then $s.z = \alpha z$, so that $\alpha^p = 1$; hence, $\alpha = 1$. This contradiction shows that s must have a unique fixed point.

Lemma 3.1. *Let $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ be nontrivial and of finite order. The following are equivalent:*

(1) *s has a unique fixed point in $\mathbb{P}^1(k)$;*
(2) *s has order $p > 0$; and*
(3) $\mathrm{Tr}(s)^2 = 4\det(s)$.

Proof. The equivalence of the first two statements was proved above. We now prove the equivalence of the first and third statements. The final statement is homogeneous and quadratic in the entries of the matrix s, so it is well defined on $\mathrm{PGL}_2(k)$. Moreover, the first and third statements are invariant under conjugation in $\mathbb{P}^1(k)$, so we may assume that s fixes ∞. Thus $\gamma = 0$. Now ∞ is the unique fixed point of s precisely when $\delta - \alpha = 0$ (see (3.1)), or equivalently, when

$$\mathrm{Tr}(s)^2 - 4\det(s) = (\alpha + \delta)^2 - 4\alpha\delta = (\delta - \alpha)^2 = 0.$$

□

Since an element s satisfying the three equivalent conditions in the lemma can be conjugated to $\left(\begin{smallmatrix} 1 & \beta \\ & 1 \end{smallmatrix}\right)$, one says that s is **unipotent**.

Lemma 3.2. *Let* $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ *be nontrivial.*

- *s has order 2 if and only if* $\mathrm{Tr}(s) = 0$.
- *s has order 3 if and only if* $\mathrm{Tr}(s)^2 = \det(s)$.
- *s has order 5 if and only if* $\mathrm{Tr}(s)^4 - 3\mathrm{Tr}(s)^2\det(s) + \det(s)^2 = 0$.

Remark 3.3. Note that the trace/determinant equations are homogeneous in the entries of s of degree 1, 2, and 4, respectively, so that their solution sets are well defined subsets of $\mathrm{PGL}_2(k)$.

Proof. In all cases, the conditions are invariant under conjugation, so we may assume that s fixes ∞. If ∞ is the only fixed point, then the previous lemma shows that $s = \left(\begin{smallmatrix} 1 & \gamma \\ & 1 \end{smallmatrix}\right)$ for some nonzero $\gamma \in k$ and s has order p. For $p = 2, 3$, the third statement of the previous lemma reduces immediately to the desired equations for the trace and determinant of s. For $p = 5$, we see that

$$\mathrm{Tr}(s)^4 - 3\mathrm{Tr}(s)^2\det(s) + \det(s)^2 = \left[\mathrm{Tr}(s)^2 - 4\det(s)\right]^2,$$

so that the desired criterion for order 5 reduces to the one in the previous lemma.

Suppose now that s has two distinct fixed points. Then we may suppose after conjugation that it fixes 0 and ∞. Hence $s = \left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$, and s has order n precisely when λ has order n (which must necessarily be prime to p). For $n = 2$, this means $\lambda = -1$, so that $\mathrm{Tr}(s) = 0$. For $n = 3$, this means $\lambda^2 + \lambda + 1 = 0$, so that

$$\mathrm{Tr}(s)^2 - \det(s) = (\lambda + 1)^2 - \lambda = 0.$$

For $n = 5$, it means $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 = 0$, so that

$$\mathrm{Tr}(s)^4 - 3\mathrm{Tr}(s)^2\det(s) + \det(s)^2 = (\lambda + 1)^4 - 3\lambda(\lambda + 1)^2 + \lambda^2 = 0.$$

□

4. Special subgroups

Convention. Throughout this section we will assume k is an algebraically closed field.

4.1. **Cyclic subgroups.** If $s \in \mathrm{PGL}_2(k)$ is nontrivial, then it fixes at least one point of $\mathbb{P}^1(k)$, which we may assume is ∞ after a suitable conjugation. If ∞ is the only fixed point of s, then $s = \left(\begin{smallmatrix} 1 & \beta \\ & 1 \end{smallmatrix}\right)$, and it generates a cyclic group of order p (Lemma 3.1). Moreover, we see that $\left(\begin{smallmatrix} \beta^{-1} & \\ & 1 \end{smallmatrix}\right) s \left(\begin{smallmatrix} \beta & \\ & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$, and hence every cyclic subgroup of order p is conjugate to $\langle \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) \rangle$ inside $\mathrm{PGL}_2(k)$.

Now suppose that s fixes two distinct points of $\mathbb{P}^1(k)$. After a suitable conjugation, we may assume that s fixes 0 and ∞. Hence $s = \left(\begin{smallmatrix} \alpha & \\ & 1 \end{smallmatrix}\right)$. If $\alpha^m \neq 1$ for any $m \neq 0$, then s has infinite order and generates a subgroup isomorphic to $\mathbb{Z}$. If $\alpha^m = 1$ for some $m > 1$, then α is a root of unity in k. The roots of unity in k are $\overline{\mathbb{F}}_p^\times$, and in particular, each has order prime to p. Hence s generates a p-regular cyclic subgroup of $\mathrm{PGL}_2(k)$.

Proposition 4.1. *Let G be a nontrivial finite cyclic subgroup of $\mathrm{PGL}_2(k)$. Then exactly one of the following is true:*

(1) *$|G| = p$, it fixes a unique point of $\mathbb{P}^1(k)$, and G is conjugate to $\left(\begin{smallmatrix} 1 & \mathbb{F}_p \\ & 1 \end{smallmatrix}\right)$; or*
(2) *G is p-regular, it fixes exactly two of points of $\mathbb{P}^1(k)$, and G is conjugate to $\left(\begin{smallmatrix} \Lambda & \\ & 1 \end{smallmatrix}\right)$ for some cyclic subgroup $\Lambda \subset \overline{\mathbb{F}}_p^\times \subset k^\times$.*

In particular, the order of a finite cyclic group uniquely determines its conjugacy class in $\mathrm{PGL}_2(k)$.

Proof. We have already proved everything but the final statement about conjugacy classes. If $|G| = p$, then it is conjugate to $\left(\begin{smallmatrix} 1 & \mathbb{F}_p \\ & 1 \end{smallmatrix}\right)$, so that any cyclic group of order p lies in the same conjugacy class. If $p \nmid |G|$, then it is conjugate to $\left(\begin{smallmatrix} \Lambda & \\ & 1 \end{smallmatrix}\right)$ for some finite cyclic group $\Lambda \subset \overline{\mathbb{F}}_p^\times$. For some q, Λ is contained in the multiplicative group $\mathbb{F}_q^\times$. The latter is a cyclic group, and so it has a unique subgroup of any order dividing $q-1$. That is, the order of G uniquely determines Λ, and hence also the $\mathrm{PGL}_2(k)$-conjugacy class of G. □

Another normal form for p-regular cyclic subgroups will be useful when we pass to non-algebraically closed fields.

Corollary 4.2. *Let G be a finite p-regular cyclic subgroup of $\mathrm{PGL}_2(k)$ of order $n \geq 3$, and let ζ be a primitive n-th root of unity. Then G is conjugate to the subgroup generated by $\left(\begin{smallmatrix} \lambda+1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$, where $\lambda = \zeta + \zeta^{-1}$.*

Proof. The elements $\left(\begin{smallmatrix} \lambda+1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right)$ are conjugate:

$$\begin{pmatrix} 1 & -\zeta^{-1} \\ 1 & -\zeta \end{pmatrix}^{-1} \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & -\zeta^{-1} \\ 1 & -\zeta \end{pmatrix} = \begin{pmatrix} \lambda+1 & -1 \\ 1 & 1 \end{pmatrix}.$$

□

4.2. **p-subgroups.** In this section, we will assume $\mathrm{char}(k) = p > 0$. Suppose $G \subset \mathrm{PGL}_2(k)$ is a nontrivial p-group, and let $s \in G$ be any nontrivial element. We saw above that s must fix a unique point of $\mathbb{P}^1(k)$, so after conjugating G if necessary, we may assume that s fixes ∞. We claim now that every element of G fixes ∞. Suppose not, and select $s' \in G \smallsetminus \{I, s\}$ that fixes a (unique) point $x \neq \infty$. After conjugating G by $\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right)$, we may assume that s' fixes 0 and s still fixes ∞. So $s = \left(\begin{smallmatrix} 1 & \beta \\ & 1 \end{smallmatrix}\right)$ and $s' = \left(\begin{smallmatrix} 1 & \\ \beta' & 1 \end{smallmatrix}\right)$ for some $\beta, \beta' \in k^\times$. Since G is a p-group, it follows that ss' must fix a unique point as well. Lemma 3.1 shows that

$$\mathrm{Tr}(ss')^2 - 4\det(ss') = \beta\beta'(4 + \beta\beta') = 0.$$

When $p = 2$, this contradicts $\beta\beta' \neq 0$. When $p > 2$, we find that $s^2 s' \in G$ as well, but that

$$\mathrm{Tr}(s^2 s') - 4\det(s^2 s') = 4\beta\beta'(2 + \beta\beta') \neq 0.$$

This contradiction completes the proof that every element of G fixes ∞. We have proved the following lemma.

Lemma 4.3. *If $G \subset \mathrm{PGL}_2(k)$ is a nontrivial p-group, then G is conjugate to a group of the form $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$, where Γ is an additive subgroup of k (and hence an $\mathbb{F}_p$-vector space). In particular, G fixes a unique point of $\mathbb{P}^1(k)$.*

Now suppose that G and G' are two finite p-groups in $\mathrm{PGL}_2(k)$. To determine necessary and sufficient conditions for these two subgroups to be conjugate, it suffices to assume that $G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ and $G' = \left(\begin{smallmatrix} 1 & \Gamma' \\ & 1 \end{smallmatrix}\right)$ for some additive subgroups Γ and Γ' inside k. If there exists $u \in \mathrm{PGL}_2(k)$ so that $uGu^{-1} = G'$, then u must fix ∞, so that $u = \left(\begin{smallmatrix} \alpha & \beta \\ & 1 \end{smallmatrix}\right)$. Hence

$$sGs^{-1} = \begin{pmatrix} \alpha & \beta \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}\beta \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha\Gamma \\ & 1 \end{pmatrix},$$

which implies that $\Gamma' = \alpha\Gamma$. This calculation shows that $\alpha\Gamma = \Gamma'$ for some $\alpha \in k^\times$ is a necessary and sufficient condition to have G and G' be conjugate.

Proposition 4.4. *The conjugacy classes of finite p-subgroups of* $\mathrm{PGL}_2(k)$ *are in bijective correspondence with the finite additive subgroups of k modulo homotheties.*

To close this section, we define the **stabilizer**[3] of a finite additive subgroup $\Gamma \subset k$ to be

$$\mathbb{F}_\Gamma = \{\alpha \in k : \alpha\Gamma \subset \Gamma\}.$$

Then one verifies easily that $\mathbb{F}_\Gamma$ is a subfield of k. Moreover, each nonzero element of $\mathbb{F}_\Gamma$ induces an $\mathbb{F}_p$-linear automorphism of Γ, and since Γ is finite, there are only finitely many possibilities in total for such an automorphism. Hence $\mathbb{F}_\Gamma$ is a finite subfield of k. Observe further that for any $\alpha \in k^\times$, we have $k_{\alpha\Gamma} = \mathbb{F}_\Gamma$, so that the stabilizer is a homothety class invariant.

Proposition 4.5. *If G is a finite p-subgroup of* $\mathrm{PGL}_2(k)$*, then G is conjugate to* $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ *for some additive group* Γ *such that* $\mathbb{F}_\Gamma \subset \Gamma \subset k$*.*

Proof. We have already shown G is conjugate to a group of the form $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ above. For $\gamma \in \Gamma \smallsetminus \{0\}$, observe that

$$\begin{pmatrix} 1 & \gamma^{-1} \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \gamma^{-1}\Gamma \\ & 1 \end{pmatrix}.$$

The group $\gamma^{-1}\Gamma$ contains the element $1 \in k$; let us replace Γ with $\gamma^{-1}\Gamma$. Then $\alpha = \alpha.1 \in \Gamma$ for each α in the stabilizer field $\mathbb{F}_\Gamma$. □

4.3. **Subgroups stabilizing a pair of points.** Let G be a finite subgroup of $\mathrm{PGL}_2(k)$ that stabilizes a pair of points, but does not fix them. After conjugation, we may assume that G stabilizes $\{0, \infty\}$. Define

$$H = \{s \in G : s.\infty = \infty \text{ and } s.0 = 0\}.$$

We saw in §4.1 that H is cyclic and generated by an element $\left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$. We observe that H is normal in G. Indeed, it is invariant under conjugation by any element fixing both 0 and ∞ as these are precisely the elements of H. Any element of G that stabilizes the set $\{0, \infty\}$ without fixing it pointwise must be of the form $t = \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$ for some $\tau \in k^\times$. We find that

$$t \begin{pmatrix} \lambda & \\ & 1 \end{pmatrix} t^{-1} = \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} \begin{pmatrix} \lambda & \\ & 1 \end{pmatrix} \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} = \begin{pmatrix} \lambda^{-1} & \\ & 1 \end{pmatrix}.$$

Hence H is normal. In fact, this computation also shows that the subgroup of G generated by H and t is dihedral.

We now prove that G is generated by H and t. We may conjugate G by $\left(\begin{smallmatrix} \sqrt{\tau^{-1}} & \\ & 1 \end{smallmatrix}\right)$ in order to assume that $t = \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$; note that this operation does not affect H. We have already shown that $G \smallsetminus H$ consists of elements of the form $\left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$. Suppose we have such an element. Then $\left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) = \left(\begin{smallmatrix} \tau & \\ & 1 \end{smallmatrix}\right) \in H$. If λ has order $n = |H|$, then $\tau^n = 1$, which means there are at most n such elements in G. On the other hand, we can generate n elements of this shape via

$$\begin{pmatrix} \lambda^j & \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = \begin{pmatrix} & \lambda^j \\ 1 & \end{pmatrix}, \quad j = 1, \ldots, n.$$

Hence G is generated by H and t as desired.

Proposition 4.6. *Let* $G \subset \mathrm{PGL}_2(k)$ *be a finite subgroup that stabilizes a pair of points of* $\mathbb{P}^1(k)$*. Then up to* $\mathrm{PGL}_2(k)$*-conjugacy, G satisfies one of the following:*

[3]The multiplicative group $k^\times$ acts on the set of all finite additive subgroups of k, and the stabilizer (in the usual sense of a group action) of a particular such subgroup Γ is precisely $\mathbb{F}_\Gamma^\times$. Dickson prefers to call $\mathbb{F}_\Gamma$ the **multiplier** [3, §70].

(1) $G = \left(\begin{smallmatrix} \Lambda & \\ & 1 \end{smallmatrix}\right)$ *for some (cyclic) subgroup* $\Lambda \subset \overline{\mathbb{F}}_p^\times$*; in this case,* G *fixes a pair of points of* $\mathbb{P}^1(k)$.
(2) $G = \left(\begin{smallmatrix} \Lambda & 0 \\ & 1 \end{smallmatrix}\right) \rtimes \langle \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) \rangle$ *for some (cyclic) subgroup* $\Lambda \subset \overline{\mathbb{F}}_p^\times$ *so that* G *is dihedral; in this case,* G *stabilizes a pair of points, but does not fix them.*

In either case, we observe that G *is uniquely determined up to* $\mathrm{PGL}_2(k)$*-conjugacy by its order and whether or not it fixes the pair of points or swaps them.*

To conclude this section, let us suppose that G is a finite subgroup of $\mathrm{PGL}_2(k)$, and let H be a nontrivial maximal p-regular cyclic subgroup. We showed above that H fixes a pair of points $\{x, y\} \subset \mathbb{P}^1(k)$. If $s \in G$ lies in the normalizer of H, then for each nontrivial $h \in H$, there is $h' \in H$ such that $shs^{-1} = h'$. Now observe that

$$h's.x = sh.x = s.x \qquad h's.y = sh.y = s.y,$$

so that $s.x$ and $s.y$ are fixed points of h'. This means s stabilizes the pair $\{x, y\}$. If s fixes both of these points, then $s \in H$ by maximality; otherwise, s swaps x and y. It follows that the normalizer $N_G(H)$ consists of all elements of G that stabilize the pair of points $\{x, y\}$, so that our above work proves $N_G(H) = H$ or $N_G(H)$ is dihedral with maximal cyclic subgroup H (of index 2).

Proposition 4.7. *Let* G *be a finite subgroup of* $\mathrm{PGL}_2(k)$*, and let* H *be a nontrivial maximal* p*-regular cyclic subgroup. Then the normalizer of* H *satisfies* $[N_G(H) : H] = 1$ *or* 2*, and in the latter case it is dihedral.*

4.4. **Subgroups fixing a unique point.** The goal of this section is to prove the following result:

Proposition 4.8. *Suppose* G *is a finite subgroup of* $\mathrm{PGL}_2(k)$ *that fixes a unique point of* $\mathbb{P}^1(k)$*. Then* k *has positive characteristic* p*, and up to conjugation in* $\mathrm{PGL}_2(k)$*, there exist a nontrivial additive subgroup* $\Gamma \subset k$ *and an integer* $n \in \mathbb{N} \smallsetminus p\mathbb{N}$ *satisfying* $\mu_n(k) \subset \mathbb{F}_\Gamma^\times \subset \Gamma \smallsetminus \{0\}$ *and*

$$G = \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix}.$$

(Recall that $\mathbb{F}_\Gamma = \{\alpha \in k : \alpha\Gamma \subset \Gamma\}$*.) The group* G *is determined up to* $\mathrm{PGL}_2(k)$*-conjugation by* n *and the homothety class* $\{\alpha\Gamma : \alpha \in k^\times\}$*.*

Remark 4.9. With the notation of the proposition, let e be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathbb{F}_{p^e}$ is the smallest extension of $\mathbb{F}_p$ containing $\mu_n(k)$, and hence we may assume that $\mathbb{F}_{p^e} \subset \mathbb{F}_\Gamma \subset \Gamma$.

Corollary 4.10. *If* G *is a finite subgroup of* $\mathrm{PGL}_2(k)$*, then* G *fixes a unique point of* $\mathbb{P}^1(k)$ *if and only if* G *is* p*-semi-elementary, where* $p = \mathrm{char}(k) > 0$*.*

Proof. One implication follows immediately from the preceding proposition. For the other, G is p-semi-elementary if and only if it fits into an exact sequence $1 \to P \to G \to G/P \to 1$ with P a p-group and G/P cyclic of order prime to p. We saw in §4.2 P must fix a unique point of $\mathbb{P}^1(k)$, and so must any group that normalizes it. □

Corollary 4.11. *Suppose* G *is a finite subgroup of* $\mathrm{PGL}_2(k)$ *of order* $p^r(p^r - 1)$ *that fixes a unique point of* $\mathbb{P}^1(k)$*. Then* G *is* $\mathrm{PGL}_2(k)$*-conjugate to* $B(\mathbb{F}_{p^r})$*.*

Proof. The proposition shows that we may assume $G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_{p^r-1}(k) & \\ & 1 \end{smallmatrix}\right)$, where Γ is an additive subgroup of k of order p^r containing $\mu_{p^r-1}(k)$. The group $\mu_{p^r-1}(k)$ agrees with the multiplicative group $\mathbb{F}_{p^r}^\times$, so that $\Gamma = \mathbb{F}_{p^r}$. □

We now begin the proof of the proposition. Write $B(k)$ for the **standard Borel subgroup** of $\mathrm{PGL}_2(k)$:

$$B(k) = \{s \in \mathrm{PGL}_2(k) : s.\infty = \infty\} = \left\{ \begin{pmatrix} \alpha & \beta \\ & 1 \end{pmatrix} : \alpha \in k^\times, \beta \in k \right\}.$$

We also write $U(k)$ for the unipotent subgroup of $B(k)$ (i.e., those elements with $\alpha = 1$). Note that $U(k)$ is an abelian group, and it can be written concretely as $U(k) = \left(\begin{smallmatrix} 1 & k \\ & 1 \end{smallmatrix}\right)$. Moreover, we find that

$$\begin{pmatrix} \alpha & \beta \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}\beta \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha\gamma \\ & 1 \end{pmatrix}, \tag{4.1}$$

so that $U(k)$ is a normal subgroup of $B(k)$.

More generally, any subgroup conjugate to $B(k)$ will be called a Borel subgroup. Equivalently, a Borel subgroup may be characterized as the set of all elements of $\mathrm{PGL}_2(k)$ fixing a particular point of $\mathbb{P}^1(k)$.

There is an exact sequence of homomorphisms

$$0 \to U(k) \to B(k) \xrightarrow{\pi} k^\times \to 1,$$

where π maps an element $s = \left(\begin{smallmatrix} \alpha & \beta \\ & 1 \end{smallmatrix}\right)$ to the derivative of $s.z = \alpha z + \beta$. (Note that this is well defined independent of the matrix representation of s.) For any subgroup $G \subset \mathrm{PGL}_2(k)$, we write $B_G = B(k) \cap G$ and $U_G = U(k) \cap G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ for some additive subgroup $\Gamma \subset k$. Then the above exact sequence descends to an exact sequence

$$0 \to U_G \to B_G \xrightarrow{\pi} \pi(B_G) \to 1.$$

If $\pi(B_G)$ is cyclic, then π has a section, and we may represent B_G as an abstract semidirect product $B_G \cong \Gamma \rtimes \pi(B_G)$. This is the case, for example, if G is a finite group, so that $\pi(B_G) \subset \mu_n(k)$ for some $n \geq 1$. More intrinsically, let S_G be the image of a section of π. Then S_G is generated by an element $s = \left(\begin{smallmatrix} \lambda & \eta \\ & 1 \end{smallmatrix}\right)$, and we have

$$B_G = \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \langle s \rangle.$$

Note that if s is nontrivial, then $\lambda \neq 1$ (else $s \in U_G$).

Suppose now that G is a finite subgroup of $\mathrm{PGL}_2(k)$ that fixes a unique point of $\mathbb{P}^1(k)$. As usual, we may assume that G fixes ∞ after a suitable conjugation, so that $G \subset B(k)$. Moreover, let us write $U_G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ and choose an element s as above so that $G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \langle s \rangle$. Now s fixes ∞ and at least one other point of $\mathbb{P}^1(k)$. (It fixes exactly one other point if s is nontrival.) Note that $\Gamma \neq 0$, else G fixes at least two points. In particular, the characteristic of k is positive. After conjugating G by an element of $U(k)$, we may assume that s fixes 0, so that it is of the form $s = \left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$. That is, $\langle \lambda \rangle = \mu_n(k)$ for some n coprime to p, and $G = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$.

Now observe that, with λ as above and $\gamma \in \Gamma$, we have

$$\begin{pmatrix} \lambda & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda\gamma \\ & 1 \end{pmatrix} \in G,$$

so that $\lambda\Gamma \subset \Gamma$. That is, $\mu_n(k) \subset \mathbb{F}_\Gamma^\times$. After a further conjugation if necessary, we may assume that $\mu_n(k) \subset \mathbb{F}_\Gamma^\times \subset \Gamma$ (Proposition 4.5).

Finally we must deal with the question of conjugacy of these subgroups. Let $G, G' \subset \mathrm{PGL}_2(k)$ be finite subgroups of the following form:

$$G = \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix} \qquad G' = \begin{pmatrix} 1 & \Gamma' \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_{n'}(k) & \\ & 1 \end{pmatrix},$$

where $n, n' \in \mathbb{N} \smallsetminus p\mathbb{N}$ and $\Gamma, \Gamma' \subset k$ are finite additive subgroups. Suppose first that they are conjugate; i.e., there is $s \in \mathrm{PGL}_2(k)$ such that $sGs^{-1} = G'$. Then s must fix ∞, so that $s = \left(\begin{smallmatrix} \alpha & \beta \\ & 1 \end{smallmatrix}\right)$.

Since $sU_Gs^{-1} = U_{G'}$, our work in §4.2 shows that $\Gamma' = \alpha\Gamma$. Comparing the orders of G and G' shows $n = n'$.

Conversely, suppose that G and G' are as above, that $\Gamma' = \alpha\Gamma$, and $n = n'$. For $\gamma \in \Gamma$ and $\lambda \in \mu_n(k)$, we have

$$\begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} \begin{pmatrix} \lambda & \gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} \lambda & \alpha\gamma \\ & 1 \end{pmatrix} \in G'.$$

As G and G' have the same order, it follows that G and G' are conjugate. This completes the proof of the proposition.

4.5. **Tetrahedral subgroups.** Recall that the group of orientation-preserving symmetries of a regular tetrahedron is isomorphic to $\mathfrak{A}_4$. (Look at the action of the symmetry group on the four vertices of the tetrahedron.) Any group isomorphic to $\mathfrak{A}_4$ will therefore be called **tetrahedral**.

Lemma 4.12. *Let G be a non-abelian group of order 12 possessing a normal Klein 4-subgroup. Then G is of tetrahedral type.*

Proof. Let $N = \{e, n_1, n_2, n_3\}$ be the given normal subgroup, let $h \in G$ be an element of order 3, and let $H = \langle h \rangle$. Then $N \cap H = \emptyset$ and $NH = G$. We observe that $hNh^{-1} = N$, so that $hn_ih^{-1} = n_j$ for some j. If conjugation by h fixes all n_i, then we would find that G is abelian. If conjugation by h fixed only one n_i and permuted the other 2, then h would have order 2. So h permutes the n_i cyclically. Hence $G = N \rtimes H$, and the action $H \to \mathrm{Aut}(N)$ is given by cyclic permutation on the three nontrivial elements of N. One now checks that $\mathfrak{A}_4$ may also be written as a semidirect product of the normal subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$ (containing all elements of order 2) and the subgroup generated by (123); hence, it is isomorphic to G. □

Proposition 4.13. *If $p = 2$ and G is a tetrahedral subgroup of $\mathrm{PGL}_2(k)$, then G is conjugate to the standard Borel subgroup $B(\mathbb{F}_4) = \left(\begin{smallmatrix} 1 & \mathbb{F}_4 \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mathbb{F}_4^\times & \\ & 1 \end{smallmatrix}\right)$.*

Proof. We know G contains a normal 4-group N, each nontrivial element of which must be unipotent since $p = 2$. After conjugating G if needed, we may assume that $N = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ for some $\Gamma \subset k$ of rank 2 (Lemma 4.3). By normality, if $s \in G$ and $u \in N$, then there is $u' \in N$ such that $su = u's$. Since ∞ is the unique fixed point of each nontrivial element of N, we have

$$s.\infty = s(u.\infty) = u'(s.\infty) \;\Rightarrow\; s.\infty = \infty.$$

That is, G fixes ∞, or equivalently $G \subset B(k)$. The order of G is $12 = 2^2(2^2 - 1)$. Apply Corollary 4.11. □

Proposition 4.14. *Suppose $p > 2$ and let G be a tetrahedral subgroup of $\mathrm{PGL}_2(k)$. Then G is conjugate to the semidirect product $N \rtimes C$, where $N = \left\{\left(\begin{smallmatrix} \pm 1 & \\ & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \\ & \pm 1 \end{smallmatrix}\right)\right\}$, and C is the cyclic group of order 3 generated by $\begin{pmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{pmatrix}$. In particular, any two tetrahedral subgroups of $\mathrm{PGL}_2(k)$ are conjugate when $\mathrm{char}(k)$ is odd.*

Proof. A tetrahedral group contains a normal 4-group N. Let s_1 be a nontrivial element of N, and let us conjugate G so that s_1 fixes 0 and ∞. (Here we have used the hypothesis $p \neq 2$.) If $s_2 \in N$ is another element of order 2, then it must commute with s_1, so that

$$s_1s_2.0 = s_2s_1.0 = s_2.0 \qquad s_1s_2.\infty = s_2s_1.\infty = s_2.\infty.$$

Hence s_2 stabilizes the set $\{0, \infty\}$, and it cannot fix these elements since s_1 is the only element of order 2 with this property. Repeating this argument for the third nontrivial element of N shows that there exist $\tau \neq \tau' \in k^\times$ such that

$$N = \left\{I, \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} & \tau \\ 1 & \end{pmatrix}, \begin{pmatrix} & \tau' \\ 1 & \end{pmatrix}\right\}.$$

After conjugating by $\begin{pmatrix} \sqrt{\tau^{-1}} & \\ & 1 \end{pmatrix}$, we may assume that $\tau = 1$. Since N is abelian, we have

$$\begin{pmatrix} 1 & \\ & \tau' \end{pmatrix} = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} & \tau' \\ 1 & \end{pmatrix} = \begin{pmatrix} & \tau' \\ 1 & \end{pmatrix} \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = \begin{pmatrix} \tau' & \\ & 1 \end{pmatrix}.$$

Hence $(\tau')^2 = 1$, or $\tau' = -1$, and N is of the form claimed in the statement of the proposition.

The group G has normal subgroup N and four conjugate subgroups of order 3. In particular, every element of $G \smallsetminus N$ has order 3. We now compute the set of all elements of $\mathrm{PGL}_2(k)$ of order 3 that normalize N. Suppose $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is such an element. Then

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} -(\alpha\delta + \beta\gamma) & 2\alpha\beta \\ -2\gamma\delta & \alpha\delta + \beta\gamma \end{pmatrix}.$$

For s to be a normalizer, we must have either

$$\alpha\beta = \gamma\delta = 0, \text{ or} \tag{4.2}$$

$$\alpha\delta = -\beta\gamma \quad \text{and} \quad \alpha\beta = \pm\gamma\delta \quad \text{and} \quad \alpha\beta\gamma\delta \neq 0. \tag{4.3}$$

Let us suppose first that (4.2) holds. Then either $\alpha = \delta = 0$ or $\beta = \gamma = 0$. In the former case, s has order 3 if and only if $\mathrm{Tr}(s)^2 - \det(s) = -\det(s) = 0$, so that this cannot occur (Lemma 3.2). In the latter case, we may assume $\delta = 1$, so that s has order 3 precisely when $\alpha^3 = 1$ and $\alpha \neq 1$. But observe that

$$\begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} & \alpha^2 \\ 1 & \end{pmatrix} \notin N,$$

so that the full subgroup N is not stable under conjugation by s. Hence (4.2) may discarded.

Let us now suppose that (4.3) holds, so that $\beta\gamma = -\alpha\delta$. By Lemma 3.2, if s has order 3, then

$$0 = \mathrm{Tr}(s)^2 - \det(s) = (\alpha + \delta)^2 - \alpha\delta + \beta\gamma = \alpha^2 + \delta^2.$$

Hence $\delta = \pm i\alpha$, where we have chosen i to be a fixed square root of -1 for ease of notation. Squaring both sides of the second equation in (4.3) and dividing by $\alpha^2 = -\delta^2$, we see that $\beta^2 = -\gamma^2$. Without loss of generality, we may suppose that $\gamma = 1$, so that $\beta = \pm i$. Squaring both sides of the first equation in (4.3) and replacing δ^2 with $-\alpha^2$ and β^2 with $-\gamma^2 = -1$, we find that $\alpha^4 = 1$. We conclude that $s = \begin{pmatrix} \epsilon_1 & \beta \\ 1 & \epsilon_2 \end{pmatrix}$, where $\epsilon_j^4 = 1$ for $j = 1, 2$ and $\beta = \pm i$. In order for the first equation of (4.3) to be satisfied, we must have $\beta = -\epsilon_1\epsilon_2$, so that exactly one of ϵ_1 and ϵ_2 is a primitive fourth root of unity, while the other is ± 1. Hence the elements of order 3 that normalize N lie in the following set:

$$\left\{ \begin{pmatrix} \epsilon & -\epsilon\epsilon' i \\ 1 & \epsilon' i \end{pmatrix} \ : \ \epsilon^2 = (\epsilon')^2 = 1 \right\} \cup \left\{ \begin{pmatrix} \epsilon i & -\epsilon\epsilon' i \\ 1 & \epsilon' \end{pmatrix} \ : \ \epsilon^2 = (\epsilon')^2 = 1 \right\}.$$

As there are 8 elements in this set, and since a tetrahedral group has 8 elements of order 3, we have found all of them.

Let $s \in G$ be any element of order 3. Evidently $N \cup Ns \cup Ns^2 = G$, so that $G = N \rtimes \langle s \rangle$. Now choose $\epsilon = 1$ and $\epsilon' = -1$ in the first of the above sets of elements of order 3 to arrive at the desired generator G. □

Corollary 4.15. *If $p = 3$ and $G \subset \mathrm{PGL}_2(k)$ is octahedral, then G is conjugate to $\mathrm{PSL}_2(\mathbb{F}_3)$.*

Proof. The group $\mathrm{PSL}_2(\mathbb{F}_3)$ acts faithfully on the set $\mathbb{P}^1(\mathbb{F}_3)$, which has only four points. This gives an injective homomorphism $\mathrm{PSL}_2(\mathbb{F}_3) \to \mathfrak{S}_4$. By comparing orders, we see that image in $\mathfrak{S}_4$ has index 2, which means $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$. Thus $\mathrm{PSL}_2(\mathbb{F}_3)$ is tetrahedral, and the preceding proposition shows G and $\mathrm{PSL}_2(\mathbb{F}_3)$ must be conjugate. □

4.6. **Octahedral subgroups.** Recall that the group of orientation-preserving symmetries of a regular octahedron is isomorphic to $\mathfrak{S}_4$. (Look at the action of the symmetry group on the set of pairs of opposite faces, of which there are four.) Any group isomorphic to $\mathfrak{S}_4$ will therefore be called **octahedral**.

Lemma 4.16. *Let G be a group of order 24 such that (i) G has no central element of order 2, and (ii) G has a complete set of 4 conjugate cyclic subgroups of order 3, each of which has normalizer equal to a dihedral subgroup of order 6. Then G is of octahedral type (i.e., $G \cong \mathfrak{S}_4$).*

Proof. Let $C_1, \ldots, C_4$ be the four conjugate cyclic subgroups of order 3, and let $D_1, \ldots, D_4$ be the associated dihedral normalizers. Note that the D_i must also be conjugate. Consider the action of G on the set $\{C_1, \ldots, C_4\}$ given by conjugation; it induces a homomorphism $\phi : G \to \mathfrak{S}_4$. We wish to show that ϕ is injective. Suppose that $\phi(g) = e$. Then $gC_ig^{-1} = C_i$ for each i, so that $g \in D_1 \cap \cdots \cap D_4$. If g is of order 3, then it belongs to each of the C_i, and hence the C_i are not distinct, a contradiction. If $D_1 \cap \cdots \cap D_4$ contains a pair of distinct elements of order 2, then it contains their product, which has order 3, another contradiction. If the intersection contains a single element of order 2, say g, then sgs^{-1} lies in the intersection as well for every $s \in G$. Hence $sgs^{-1} = g$, or g lies in the center of G, a final contradiction. We deduce that ϕ is injective, so that $G \cong \mathfrak{S}_4$. □

Proposition 4.17. *Suppose $p > 2$ and $G \subset \mathrm{PGL}_2(k)$ is an octahedral subgroup. Then up to conjugation, G is generated by the tetrahedral subgroup $T = N \rtimes C$ given by Proposition 4.14 and the element $\left(\begin{smallmatrix} \sqrt{-1} & \\ & 1 \end{smallmatrix}\right)$ of order 4. In particular, any two octahedral subgroups of $\mathrm{PGL}_2(k)$ are conjugate when $\mathrm{char}(k)$ is odd.*

Remark 4.18. When $p = 2$, we know that every element of finite order in $\mathrm{PGL}_2(k)$ has order 2 or odd order (Proposition 4.1). It follows that $\mathrm{PGL}_2(k)$ does not contain an octahedral subgroup since such groups have elements of order 4.

Proof. Evidently G contains a tetrahedral subgroup T, so after conjugation, we may assume it is of the form $T = N \rtimes C$ as in Proposition 4.14. Since $[G : T] = 2$, to generate G it suffices to produce a single element of order 4. Suppose s is such an element. Then s^2 has order 2 and corresponds to an even permutation in $\mathfrak{S}_4$, so that it lies in N. Moreover, s must commute with this element. We also see that there are three Sylow 2-subgroups of order 8, and each of them must contain a single nontrivial element of N. So let us suppose further that s is an order 4 element such that $s^2 = \left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right)$. Now s fixes two points of $\mathbb{P}^1(k)$, and its square fixes the same two points. Hence $s = \left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$ for some $\lambda \in k^\times$. To have order 4, we must have $\lambda = \sqrt{-1}$. □

Corollary 4.19. *If $p = 3$ and $G \subset \mathrm{PGL}_2(k)$ is octahedral, then G is conjugate to $\mathrm{PGL}_2(\mathbb{F}_3)$.*

Proof. The group $\mathrm{PGL}_2(\mathbb{F}_3)$ acts faithfully on the set $\mathbb{P}^1(\mathbb{F}_3)$, which has only four points. This gives an injective homomorphism $\mathrm{PGL}_2(\mathbb{F}_3) \to \mathfrak{S}_4$. As these groups have the same order, they must be isomorphic. Thus $\mathrm{PGL}_2(\mathbb{F}_3)$ is octahedral, and the preceding proposition shows G and $\mathrm{PGL}_2(\mathbb{F}_3)$ must be conjugate. □

4.7. **Icosahedral subgroups.** Recall that the group of orientation-preserving symmetries of a regular icosahedron is isomorphic to $\mathfrak{A}_5$. (See [2, §3·6–3·7].) Any group isomorphic to $\mathfrak{A}_5$ will therefore be called **icosahedral**.

Lemma 4.20. *Let G be a group of order 60 with exactly ten conjugate 3-subgroups and exactly fifteen elements of order 2 lying in five conjugate Klein 4-groups. Then G is icosahedral.*

Proof. Let $K_1, \ldots, K_5$ be the conjugate Klein 4-subgroups. We let G act on the set $\{K_1, \ldots, K_5\}$ by conjugation, so that we have a homomorphism $\phi : G \to S_5$. If we can show that G is injective, then it is isomorphic to an index 2 subgroup of S_5, which must be $\mathfrak{A}_5$.

First note that if N_i is the normalizer of K_i in G, then $|N_i| = 12$ by the orbit-stabilizer theorem. Each N_i is tetrahedral by Lemma 4.12. Indeed, it suffices to show that N_i is non-abelian. But if it were abelian, then it would contain a normal subgroup C_i of order 3, which would be one of at most five conjugate Sylow 3-subgroups of G. But G has ten conjugate 3-subgroups, a contradiction.

To show that ϕ is injective, we must prove that $N_1 \cap \cdots \cap N_5 = \{e\}$. Write N for this intersection. Then N is a normal subgroup of G, and hence of each N_i. Now N_i is tetrahedral, so its only normal subgroups are its trivial subgroups and K_i. No two of the N_i are equal since they contain conjugate subgroups K_i; hence $N \neq N_i$ for any i. The K_i have only the identity in common as they contain all fifteen of the elements of G of order 2. We conclude that $N \neq K_i$ for any i. So $N = \{e\}$. □

Lemma 4.21. *An icosahedral group G can be generated by two elements g, h subject to the relations $g^5 = h^2 = (gh)^3 = 1$.*

Proof. We may assume $G = \mathfrak{A}_5$. Let $g = (12345)$ and $h = (12)(34)$. Then $gh = (135)$ has order 3. Let $H = \langle g, h \rangle \subset G$. Evidently g and h have the correct relations, so it suffices to prove that $|H| = |G|$. Evidently H contains subgroups of order 3 and 5. We now show that H has a subgroup of order 4, so that $|H|$ is divisible by $4 \cdot 3 \cdot 5 = 60$. We have the following relations:

$$\begin{aligned} g^{-1}hg &= (15)(23) \\ (ghg^{-1})h(ghg^{-1}) &= (13)(25) \end{aligned}$$

These two products of 2-cycles generate a Klein 4-subgroup of H, which completes the proof. □

Proposition 4.22. *Suppose $p \neq 5$ and $G \subset \mathrm{PGL}_2(k)$ is icosahedral. For any primitive fifth root of unity $\zeta \in \overline{\mathbb{F}}_p^\times \subset k^\times$, the group G is conjugate to the group $\langle s, t \rangle$, where $s = \left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right)$ and $t = \left(\begin{smallmatrix} 1 & 1-\zeta-\zeta^{-1} \\ 1 & -1 \end{smallmatrix}\right)$. These generators satisfy $s^5 = t^2 = (st)^3 = I$. In particular, any two icosahedral subgroups of $\mathrm{PGL}_2(k)$ are conjugate when $\mathrm{char}(k) \neq 5$.*

Proof. We begin by showing that G is conjugate to a subgroup of the sort given in the proposition for *some* primitive fifth root of unity ζ; afterward, we will show that we may specify ζ. Let $s, t \in G$ be generators as in Lemma 4.21; i.e., s has order 5, t has order 2, and $(st)^3 = I$. Since $p \neq 5$, s must fix two elements of $\mathbb{P}^1(k)$. After conjugation, we may assume that $s = \left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right)$ with ζ some primitive fifth root of unity.

Since t has order 2, it may be written as $t = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right)$ (Lemma 3.2). Now

$$st = \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} = \begin{pmatrix} \zeta\alpha & \zeta\beta \\ \gamma & -\alpha \end{pmatrix}.$$

The condition for st to have order 3 is

$$0 = \mathrm{Tr}(st)^2 - \det(st) = \zeta^2\alpha^2 + \zeta(\gamma\beta - \alpha^2) + \alpha^2.$$

If $\alpha = 0$, then this implies $\det(t) = 0$. So we may assume that $\alpha = 1$. Now the previous equation becomes

$$\beta\gamma = -\frac{1}{\zeta}(\zeta^2 - \zeta + 1) = -\frac{\zeta^3 + 1}{\zeta(\zeta + 1)}. \tag{4.4}$$

As ζ is a primitive fifth root of unity, we find $\beta\gamma \neq 0$. If we conjugate G by $\left(\begin{smallmatrix} \gamma & \\ & 1 \end{smallmatrix}\right)$, then the subgroup generated by $\left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right)$ is unaffected, while

$$\begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ \gamma & -1 \end{pmatrix} \begin{pmatrix} \gamma^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \gamma\beta \\ 1 & -1 \end{pmatrix}.$$

So without loss of generality, we may assume that $\gamma = 1$. From (4.4), we find that

$$t = \begin{pmatrix} 1 & -(\zeta^2 - \zeta + 1)/\zeta \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 - \zeta - \zeta^{-1} \\ 1 & -1 \end{pmatrix}.$$

By construction, $s^5 = t^2 = (st)^3 = I$.

It remains to show that different fifth roots of unity give rise to conjugate subgroups of $\mathrm{PGL}_2(k)$. For each $i = 1, 2, 3, 4$, let

$$s_i = \begin{pmatrix} \zeta^i & \\ & 1 \end{pmatrix}, \quad t_i = \begin{pmatrix} 1 & 1 - \zeta^i - \zeta^{-i} \\ 1 & -1 \end{pmatrix}, \quad G_i = \langle s_i, t_i \rangle.$$

Evidently the symmetry $i \mapsto -i$ in t_i shows $G_1 = G_4$ and $G_2 = G_3$; in general, there are no further equalities among the G_i. If we let $\zeta = \zeta^3 - \zeta^2 + \zeta$, then a direct calculation shows that

$$\begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} s_2 \begin{pmatrix} \zeta^{-1} & \\ & 1 \end{pmatrix} = s_1^2 \in G_1 \qquad \text{and} \qquad \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} t_2 \begin{pmatrix} \zeta^{-1} & \\ & 1 \end{pmatrix} = t_1 s_1 t_1 s_1^{-1} t_1 \in G_1.$$

It follows that $\left(\begin{smallmatrix} \zeta & \\ & 1 \end{smallmatrix}\right) G_2 \left(\begin{smallmatrix} \zeta^{-1} & \\ & 1 \end{smallmatrix}\right) \subset G_1$, and since G_1 and G_2 have the same order, we have proved they are conjugate. □

Proposition 4.23. *Suppose $p = 5$ and $G \subset \mathrm{PGL}_2(k)$ is icosahedral. Then G is conjugate to $\mathrm{PSL}_2(\mathbb{F}_5)$. Moreover, we can take $s = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$ and $t = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$ as generators such that $s^5 = t^2 = (st)^3 = I$.*

Proof. The strategy is essentially the same as in the previous proposition. First we choose an element s of order 5. Since $p = 5$, this element is unipotent, and we may conjugate G so that it is of the form $\left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$. Let t be an element of order 2 such that $(st)^3 = I$ (Lemma 4.21). Write $t = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right)$. Then

$$st = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} = \begin{pmatrix} \alpha + \gamma & \beta - \alpha \\ \gamma & -\alpha \end{pmatrix}.$$

The condition for st to have order 3 is

$$\mathrm{Tr}(st)^2 - \det(st) = \alpha^2 + \beta\gamma + \gamma^2 = 0.$$

If $\gamma = 0$, then this implies $\alpha = 0$, so that $\det(t) = 0$. Hence $\gamma \neq 0$, and we may as well assume that $\gamma = 1$. The previous equation then implies $\beta = -\alpha^2 - 1$. That is, $t = \left(\begin{smallmatrix} \alpha & -\alpha^2 - 1 \\ 1 & -\alpha \end{smallmatrix}\right)$. Finally, we conjugate G by $\left(\begin{smallmatrix} 1 & -\alpha \\ & 1 \end{smallmatrix}\right)$. This does not affect the subgroup generated by s, but it does give

$$\begin{pmatrix} 1 & -\alpha \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha & -\alpha^2 - 1 \\ 1 & -\alpha \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix} = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}.$$

Hence we may assume without loss of generality that $t = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$.

We have shown that, up to $\mathrm{PGL}_2(k)$-conjugacy, we have $G = \langle \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right) \rangle \subset \mathrm{PSL}_2(\mathbb{F}_5)$. But these two groups have the same order, so that $G = \mathrm{PSL}_2(\mathbb{F}_5)$. □

5. The p-regular case

Convention. Throughout this section we will assume k is an algebraically closed field.

Our goal for this section is to prove Theorem C *when k is an algebraically closed field.*

Let $G \subset \mathrm{PGL}_2(k)$ be a finite p-regular subgroup. Any nontrivial element $s \in G$ fixes a unique pair of points $\{x_s, y_s\}$, and so there is a maximal cyclic subgroup $G(s) \subset G$ containing s, namely the set of all elements of G fixing x_s and y_s. Let $N(s)$ be its normalizer in G; then $[N(s) : G(s)] = 1$ or 2 by §4.3. By letting G act by conjugation on its maximal cyclic subgroups, we find that $G(s)$ lies in

a system of $|G|/|N(s)|$ conjugate subgroups. Let $G_1, \ldots, G_r$ be a complete set of representatives of the conjugacy classes of maximal cyclic subgroups of G. Let $d_i = |G_i| \geq 2$ and $f_i = [N_G(G_i) : G_i]$. As G is p-regular, we conclude that

$$|G| = 1 + \sum_{i=1}^{r} (d_i - 1) \frac{|G|}{d_i f_i}.$$

Dividing by $|G|$ and rearranging, we have

$$\frac{1}{|G|} = 1 - \sum_{i=1}^{r} \frac{1}{f_i} \left(1 - \frac{1}{d_i}\right), \text{ and} \tag{5.1}$$

$$d_i f_i \leq |G| \quad (i = 1, \ldots, r). \tag{5.2}$$

The summands on the right side of (5.1) have size at least $\frac{1}{2}\left(1 - \frac{1}{2}\right) = \frac{1}{4}$; as the left side is positive, we find that $r \leq 3$. In the remainder of the proof, we treat the various cases that can occur for r, f_i, d_i.

Case $r = 1$**.** If $f = 2$, then (5.1) implies $|G| = 2d/(d+1)$, which is not an integer. Hence $f = 1$, and (5.1) gives $|G| = d$. That is, G is cyclic.

Case $r = 2$**.** In this case, (5.1) becomes

$$1 - \frac{1}{|G|} = \frac{1}{f_1}\left(1 - \frac{1}{d_1}\right) + \frac{1}{f_2}\left(1 - \frac{1}{d_2}\right)$$

If $f_1 = f_2 = 1$, then the left side is smaller than 1 while the right side is ≥ 1. If $f_1 = f_2 = 2$, then (5.1) and (5.2) become

$$\frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2}, \quad \frac{2}{|G|} \leq \frac{1}{d_i}.$$

Evidently this is impossible, so we may assume without loss of generality that $f_1 = 1$ and $f_2 = 2$.

Now we find that

$$\frac{1}{|G|} = \frac{1}{d_1} + \frac{1}{2d_2} - \frac{1}{2} \leq \frac{1}{d_1} - \frac{1}{4},$$

so that $d_1 = 2$ or 3. If $d_1 = 2$, then $|G| = 2d_2$, so that G is dihedral. If $d_1 = 3$, then $1/|G| = 1/(2d_2) - 1/6$, so that $d_2 = 2$. Thus $|G| = 12$. We claim G is tetrahedral. Since $f_2 = 2$, the element of period 2 is normal inside a dihedral subgroup of order 4. In particular, G is non-abelian. The subgroups of order 2, of which there are $|G|/2f_2 = 3$ form a single conjugacy class, so that they generate a normal subgroup of order 4. Hence G is tetrahedral by Lemma 4.12.

Case $r = 3$**.** Here we must have $f_1 = f_2 = f_3 = 2$. Indeed, if $f_1 = 1$, then (5.1) becomes

$$\frac{1}{|G|} = \frac{1}{d_1} - \frac{d_2 - 1}{f_2 d_2} - \frac{d_3 - 1}{f_3 d_3} \leq \frac{1}{d_1} - \frac{1}{4} - \frac{1}{4} \leq 0,$$

an evident contradiction. So letting $f_i = 2$ for all i, (5.1) is equivalent to

$$1 + \frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3}.$$

If every $d_i \geq 3$, then the right side is at most 1 while the left is strictly larger than 1. So without loss of generality, we have $d_3 = 2$:

$$\frac{1}{2} + \frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2}.$$

If d_1 or d_2 is 2, we may take $d_2 = 2$, so that $|G| = 2d_1$ and G is dihedral. Otherwise, we have $d_1 > 2$ and $d_2 > 2$. The above equation implies that both d_1 and d_2 cannot be larger than 3. So let us suppose $d_2 = 3$. Thus

$$\frac{1}{6} + \frac{2}{|G|} = \frac{1}{d_1}.$$

Hence $d_1 < 6$. For $d_1 = 3, 4, 5$, we find $|G| = 12, 24, 60$, respectively. We treat these cases separately now.

If $d_1 = 3, d_2 = 3, d_3 = 2$, we find that G has two non-conjugate subgroups of order 3. But G has order $12 = 3 \cdot 4$, so we have contradicted the Sylow theorems.

If $d_1 = 4, d_2 = 3, d_3 = 2$, then $|G| = 24$, and G is octahedral by Lemma 4.16. Indeed, to check that G has no central element of order 2, observe that if s were such an element, then it would fix exactly two points x and y. By commutativity, the subgroups of order 3 would act on these two points, hence fixing them, and hence s lies in a cyclic subgroup containing an element of order 3, a contradiction.

If $d_1 = 5, d_2 = 3, d_3 = 2$, then G is of icosahedral type. Indeed, this follows immediately from Lemma 4.20 and the Sylow theorems.

We have now shown that the groups presented in Theorem C constitute all possible isomorphism classes of finite p-regular subgroups of $\mathrm{PGL}_2(k)$. In the previous section we constructed all of these groups and showed that they are unique up to $\mathrm{PGL}_2(k)$-conjugation.

6. Subgroups with elements of order p

Convention. Throughout this section we will assume k is an algebraically closed field.

This section is devoted to a proof of Theorem B *in the case where k is an algebraically closed field*. More precisely, the statement reduces to the following:

Theorem 6.1. *Let k be an algebraically closed field of characteristic $p > 0$.*

1. *Fix q a power of p. There is exactly one conjugacy class of subgroups isomorphic to each of $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$.*
2. *Let $n \in \mathbb{N} \smallsetminus p\mathbb{N}$. For each $m \in \mathbb{N}$ with $p^m n > 2$, the conjugacy classes of p-semi-elementary subgroups of order $p^m n$ are parameterized by the set of homothety classes of rank-m subgroups Γ satisfying $\mu_n(k) \subset \Gamma \subset k$ via the map*

$$\Gamma \mapsto \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix}.$$

3. *Suppose that $p = 2$ and n is an odd positive integer. Then there is a unique conjugacy class of dihedral subgroups of order $2n$.*
4. *If $p = 3$, then there is exactly one conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.*

Any p-irregular subgroup of $\mathrm{PGL}_2(k)$ is among the four types listed here.

Remark 6.2. Evidently the above result gives Theorem B when k is algebraically closed except perhaps when $p = 2$ and G is dihedral. But in this latter case, we observe that $(k^\times)^2 = k^\times$, and so the two statements agree.

Let us begin the proof. Suppose that $G \subset \mathrm{PGL}_2(k)$ is a finite subgroup containing an element of order p. Write $|G| = p^m n$ with $p \nmid n$ and $m \geq 1$, and fix a Sylow p-subgroup $P \subset G$. Without loss of generality, we may conjugate G so that $P = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ for some additive subgroup $\Gamma \subset k$ of rank m (§4.2). Let $N = N_G(P)$ be the normalizer of P in G; it may be characterized as the largest

subgroup of G that fixes $\infty \in \mathbb{P}^1(k)$. Indeed, every element of P fixes ∞, and

$$\begin{aligned} s \in N &\iff sus^{-1} \in P \quad (u \in P) \\ &\iff sus^{-1}.\infty = \infty \quad (u \in P) \\ &\iff u.(s^{-1}.\infty) = s^{-1}.\infty \quad (u \in P) \\ &\iff s^{-1}.\infty = \infty. \end{aligned}$$

After a suitable conjugation of G we may suppose that $N = P \rtimes \left(\begin{smallmatrix} \mu_d(k) \\ & 1 \end{smallmatrix}\right)$ for some integer d coprime to p with $\mu_d(k) \subset \mathbb{F}_\Gamma^\times \subset \Gamma \smallsetminus \{0\}$ (Proposition 4.8). Let us write $\mathbb{F}_\Gamma = \mathbb{F}_{p^\ell}$. Since $\mathbb{F}_\Gamma \subset \Gamma$, we must have $\ell \mid m$.

If P is normal, then $N = G$ is a subset of the standard Borel subgroup; we have already dealt with this case in §4.4. Now suppose that P is not normal in G, and let us count the elements of G of order p in two different ways. First, let P act on G by conjugation. If Q is another Sylow p-subgroup, then Q fixes a unique point $x \in \mathbb{P}^1(k) \smallsetminus \{\infty\}$. For $s \in P$, we have then $sQs^{-1}.(s.x) = s.x$, so that sQs^{-1} fixes $s.x$. As s varies through P, we find that $s.x$ varies over a set of $|P| = p^m$ elements, so that the orbit of Q under the conjugation action of P has cardinality p^m. Writing $f > 0$ for the number of orbits of Sylow p-subgroups distinct from P, it follows that

$$|\{s \in G : s^p = I \neq s\}| = (|P| - 1) + fp^m(|P| - 1) = (1 + fp^m)(p^m - 1), \tag{6.1}$$

and the elements of order p lie in $1 + fp^m$ conjugate Sylow p-subgroups of G. Note further that G acts on the set of Sylow p-subgroups by conjugation, and the stabilizer of P under this action is precisely N. Hence

$$|G| = |N| \cdot |1 + fp^m| = (1 + fp^m)p^m d.$$

Second, we estimate the number of elements of order p in G as follows. Let $\{s_i : i = 1, \ldots, fp^m\}$ be representatives of the nontrivial cosets of G/N, and write $s_i = \left(\begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix}\right)$. Note that $\gamma_i \neq 0$ for any i, else $s_i \in N$. If $t_{\lambda,\mu} = \left(\begin{smallmatrix} \lambda & \mu \\ & 1 \end{smallmatrix}\right) \in N$, then we have

$$s_i t_{\lambda,\mu} = \begin{pmatrix} \alpha_i\lambda & \alpha_i\mu + \beta_i \\ \gamma_i\lambda & \gamma_i\mu + \delta_i \end{pmatrix}.$$

By Lemma 3.1, $s_i t_{\lambda,\mu}$ has order p if and only if

$$(\alpha_i\lambda + \gamma_i\mu + \delta_i)^2 = 4\lambda \det(s_i). \tag{6.2}$$

For fixed s_i and λ, there are precisely ϵ_p values of $\mu \in k$ so that (6.2) is satisfied. Here $\epsilon_2 = 1$ and $\epsilon_p = 2$ for $p \geq 3$. So for a given s_i, there are at most $\epsilon_p d$ elements $t_{\lambda,\mu} \in N$ such that (6.2) is satisfied. Combining this argument with (6.1), we find that

$$(1 + fp^m)(p^m - 1) = |\{s \in G : s^p = I \neq s\}| \leq (p^m - 1) + \epsilon_p df p^m.$$

Subtracting $p^m - 1$ from both sides yields

$$\begin{aligned} fp^m(p^m - 1) \leq \epsilon_p df p^m \;&\Rightarrow\; p^m - 1 \leq \epsilon_p d \leq \epsilon_p(p^\ell - 1) \qquad (p^\ell = |\mathbb{F}_\Gamma|) \\ &\Rightarrow p^m - 1 < 2p^\ell - 1. \end{aligned} \tag{6.3}$$

If $\ell < m$, then this gives $p^{m-\ell} < 2$, which is impossible. Since $\ell \mid m$, we must have $\ell = m$.

For simplicity in what follows, let us write $q = p^m$. Now $\Gamma = \mathbb{F}_\Gamma = \mathbb{F}_q$, and $\mu_d(k) \subset \mathbb{F}_\Gamma^\times = \mathbb{F}_q^\times$. The first line of (6.3) gives

$$d \geq \frac{q - 1}{\epsilon_p}.$$

So if $p = 2$, then $\mu_d(k) = \mathbb{F}_q^\times$, and if $p > 2$, then $\mu_d(k) = \mathbb{F}_q^\times$ or $(\mathbb{F}_q^\times)^2$. We summarize what has been achieved thus far.

Lemma 6.3. *If G is a finite subgroup of $\mathrm{PGL}_2(k)$ containing an element of order p, then up to conjugation, exactly one of the following is true:*

- *$G \subset B(k)$ (in which case G is p-semi-elementary)*
- *G contains the Sylow p-subgroup $\left(\begin{smallmatrix} 1 & \mathbb{F}_q \\ & 1 \end{smallmatrix}\right)$ with normalizer $N = \left(\begin{smallmatrix} 1 & \mathbb{F}_q \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \Lambda & \\ & 1 \end{smallmatrix}\right)$, where $\Lambda = \mathbb{F}_q^\times$ or $\Lambda = (\mathbb{F}_q^\times)^2$. There exists an integer $f > 0$ such that*

$$|G| = |\Lambda|(1 + fq)q.$$

We assume in what follows that we are in the second case of the lemma, so that $f > 0$. It will also be convenient to have the following lemma at our disposal.

Lemma 6.4. *Write $G = N \sqcup s_1 N \sqcup \cdots \sqcup s_{fq} N$ as above. Then $s_i.\infty \neq s_j.\infty$ whenever $i \neq j$.*

Proof. If $s_i.\infty = s_j.\infty$, then $s_i^{-1} s_j.\infty = \infty$. By the characterization of N as the largest subgroup of G that fixes ∞, we must have $s_i^{-1} s_j \in N$, or equivalently $s_j \in s_i N$. □

6.1. **The case $\Lambda = (\mathbb{F}_q^\times)^2$.** Note that this includes the case q even. For $q = 2$ we will show that $G \cong \mathfrak{D}_{1+2f}$, a dihedral group. For $q > 2$, we will show that, perhaps after a further conjugation, we have $G \subset \mathrm{PSL}_2(\mathbb{F}_q)$. Then

$$\frac{q(fq+1)(q-1)}{\epsilon_p} = |G| \leq |\,\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{q(q^2-1)}{\epsilon_p},$$

so that $f = 1$ and $G = \mathrm{PSL}_2(\mathbb{F}_q)$.

Since $\Lambda = (\mathbb{F}_q^\times)^2$, the first inequality of (6.3) is actually an equality, which implies that for each fixed coset representative s_i, and each $\lambda \in \Lambda$, there are exactly $\epsilon_p > 0$ elements $\mu \in \mathbb{F}_q$ satisfying (6.2). In particular, each coset contains an element of order p, so after choosing new coset representatives, we may assume that each s_i has order p. After a suitable scaling, we may assume that $\det(s_i) = 1$. To say that s_i has order p means that

$$(\alpha_i + \delta_i)^2 = 4 \det(s_i) = 4.$$

Hence $\alpha_i + \delta_i = \pm 2$. Replacing s_i with $-s_i$, we may assume that $\mathrm{Tr}(s_i) = \alpha_i + \delta_i = 2$.

Write $\Lambda = \{\eta^2 : \eta \in \mathbb{F}_q^\times\}$. Then (6.2) becomes

$$(\alpha_i \eta^2 + \gamma_i \mu + 2 - \alpha_i)^2 = 4\eta^2 \iff \alpha_i(\eta^2 - 1) + \gamma_i \mu = -2 + 2\eta. \tag{6.4}$$

The right side lies in $\mathbb{F}_q$, and we know that for each choice of i and $\eta \in \mathbb{F}_q^\times$, there is an element $\mu = \mu_{i,\eta} \in \mathbb{F}_q$ satisfying the above equation. The proof now divides into several cases.

6.1.1. *The case $p > 2$.* If $p > 2$, then setting $\eta = -1$ in (6.4) shows $\gamma_i = -4/\mu_{i,-1} \in \mathbb{F}_q \smallsetminus \{0\}$. If $q > 3$, then $|\Lambda| > 1$. Choose $\eta \neq \pm 1$. Then $\alpha_i = (-2 + 2\eta - \gamma_i \mu_{i,\eta})(\eta^2 - 1)^{-1} \in \mathbb{F}_q$, and $\delta_i = 2 - \alpha_i \in \mathbb{F}_q$. Since $\det(s_i) = 1$, it follows that $\beta_i \in \mathbb{F}_q$ as well. Thus $G \subset \mathrm{PGL}_2(\mathbb{F}_q)$. But $\det(s_i) = 1$ for each i and $\det(t)$ is a square for each $t \in N$. Hence $G \subset \mathrm{PSL}_2(\mathbb{F}_q)$ as desired.

If $q = 3$, then $\Lambda = \{1\}$, and we will choose a slightly different normalization for our coset representatives. Replacing s_i with $-s_i$ allows us to assume that $\gamma_i = 1$. This also forces $\alpha_i + \delta_i = -2 = 1$. But then

$$\begin{pmatrix} \alpha_i & \beta_i \\ 1 & \delta_i \end{pmatrix} \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix} = \begin{pmatrix} \alpha_i & \beta_i - \alpha_i \\ 1 & \delta_i - 1 \end{pmatrix}.$$

The right side has vanishing trace, so that its order is 2. Since its determinant is 1, we may now assume that all of our coset representatives are of the form $s_i = \left(\begin{smallmatrix} \alpha_i & -1-\alpha_i^2 \\ 1 & -\alpha_i \end{smallmatrix}\right)$. Finally, we conjugate G by $\left(\begin{smallmatrix} 1 & -\alpha_1 \\ & 1 \end{smallmatrix}\right)$. This does not affect the subgroup N (consisting only of unipotent elements), and we have

$$\begin{pmatrix} 1 & -\alpha_1 \\ & 1 \end{pmatrix} s_i \begin{pmatrix} 1 & \alpha_1 \\ & 1 \end{pmatrix} = \begin{pmatrix} \alpha_i - \alpha_1 & -1 - (\alpha_i - \alpha_1)^2 \\ 1 & \alpha_1 - \alpha_i \end{pmatrix}.$$

So we are able to assume that $s_1 = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$, and that every element of G may be represented by a matrix with determinant 1 and lower left entry in $\mathbb{F}_3$. In particular, we may identify G with a subgroup of $\mathrm{SL}_2(k)/\{\pm I\}$. Now $s_1 s_i = \left(\begin{smallmatrix} -1 & \alpha_i \\ \alpha_i & -1-\alpha_i^2 \end{smallmatrix}\right)$, which implies $\alpha_i \in \mathbb{F}_3$. Hence every element of $G \subset \mathrm{PSL}_2(\mathbb{F}_3)$, which completes the proof in this case.

6.1.2. *The case $q = 2^m$ with $m > 1$.* Replace s_i with $\gamma_i^{-1} s_i$ for $i = 1, \ldots, 2f$ in order to assume that $\gamma_i = 1$. (Recall that $\gamma_i = 0$ would imply $s_i \in N$, contradicting our setup.) Select $\eta \in \mathbb{F}_q^\times \smallsetminus \{1\}$. For any such η and any i, (6.4) gives $\alpha_i = \mu_{i,\eta}/(\eta^2 - 1) \in \mathbb{F}_q$. Moreover, $\alpha_i + \delta_i = 0$, so that $\delta_i = -\alpha_i \in \mathbb{F}_q$. Note that this also implies each s_i has order 2.

If $s_i s_j \in N$, then $s_j \in s_i N$, so that $i = j$. So for $i \neq j$ there exist ℓ and $t_{\lambda,\mu} = \left(\begin{smallmatrix} \lambda & \mu \\ & 1 \end{smallmatrix}\right) \in N$ such that $s_i s_j = s_\ell t_{\lambda,\mu}$. It follows that

$$\alpha_\ell = s_\ell.\infty = s_\ell t_{\lambda,\mu}.\infty = s_i s_j.\infty = s_i.\alpha_j = \frac{\alpha_i\alpha_j + \beta_i}{\alpha_j - \alpha_i} = \frac{\alpha_i\alpha_j}{\alpha_j - \alpha_i} + \beta_i \frac{1}{\alpha_j - \alpha_i}.$$

Note that $\alpha_j - \alpha_i \neq 0$, else $\alpha_i = \alpha_j$, from which we deduce that $s_i.\infty = s_j.\infty$, in contradiction to Lemma 6.4. The above computation shows that $\beta_i \in \mathbb{F}_q$, and hence $G \subset \mathrm{PGL}_2(\mathbb{F}_q)$.

6.1.3. *The case $q = 2$.* Finally, suppose $q = 2$. Setting $s_0 = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$ and observing that $P = \{I, s_0\}$, our setup allows us to write $G = \bigsqcup_{i=0}^{2f} s_i P$, where each s_i has order 2. We also know that, since P is a Sylow 2-subgroup, all of the s_i are conjugate. Define

$$t_i = s_i s_0,$$

so that $G = \{t_0, \ldots, t_{2f}, s_0, \ldots, s_{2f}\}$.

We begin by noting that each t_i has order 2, and in particular no t_i conjugate to an s_j. Indeed, by hypothesis P has normalizer $P \rtimes \left(\begin{smallmatrix} (\mathbb{F}_2^\times)^2 & \\ & 1 \end{smallmatrix}\right) = P$, which shows that the number of elements of order 2 agrees with the number of Sylow-2 subgroups of G, which is $|G|/|P| = 1 + 2f$. So $s_0, \ldots, s_{2f}$ are all of the elements of order 2.

Define the set $H = \{t_i : i = 0, \ldots, 2f\}$. We now show that H is an abelian subgroup of G. First observe that $t_a s_b \notin H$ for any a, b. For there exists $u \in G$ such that $s_0 = u s_b u^{-1}$. Set $t_c = u t_a u^{-1}$. Then

$$(u t_a u^{-1})(u s_b u^{-1}) = t_c s_0 = s_c \;\Rightarrow\; t_a s_b = u^{-1} s_c u \in G \smallsetminus \{H\}.$$

Now define $s_{b'} = t_a s_b$. Then

$$t_a t_b s_0 = t_a s_b = s_{b'} = t_{b'} s_0 \;\Rightarrow\; t_a t_b = t_{b'} \in H,$$

and hence H is closed under multiplication. Next note that

$$s_0 t_a s_0^{-1} = s_0 t_a s_0 = s_0 s_a = (s_a s_0)^{-1} = t_a^{-1}. \tag{6.5}$$

Thus $t_a^{-1} \in H$ since a conjugate of t_a cannot have order 2, and hence H is closed under inversion. Finally, for $t_a, t_b \in H$, we have shown that $t_c := t_b^{-1} t_a^{-1} \in H$. It follows that

$$\begin{aligned} t_a t_b = (t_b^{-1} t_a^{-1})^{-1} = t_c^{-1} &= s_0 t_c s_0^{-1} \qquad \text{by (6.5)} \\ &= (s_0 t_b^{-1})(t_a^{-1} s_0^{-1}) \\ &= (t_b s_0)(s_0 t_a) \qquad \text{by (6.5)} \\ &= t_b t_a, \end{aligned}$$

so that H is abelian.

Since H is abelian of odd order, we may apply Theorem C (which we have already proved in the algebraically closed setting) to conclude that H is cyclic. If $t := t_a$ is a generator, then $G = \langle t, s_0 \rangle$. Now (6.5) gives $s_0 t s_0 = t^{-1}$, which is precisely the relation that defines a dihedral group. So $G \cong \mathfrak{D}_{1+2f}$.

6.2. **The case $\Lambda = \mathbb{F}_q^\times$, q odd.** Suppose now that $\Lambda = \mathbb{F}_q^\times$. Then $|G| = q(q-1)(1+fq)$ with $f > 0$. Observe that $\left(\begin{smallmatrix} \Lambda & \\ & 1 \end{smallmatrix}\right)$ is the maximal subgroup of G fixing 0 and ∞. For if $\left(\begin{smallmatrix} \alpha & \\ & 1 \end{smallmatrix}\right) \in G$, then

$$\begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha\Gamma \\ & 1 \end{pmatrix}.$$

Since $P = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ is a maximal p-subgroup, we must have $\alpha\Gamma = \Gamma$, so that $\alpha \in \mathbb{F}_q^\times$.

Let $t_0 = \left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right) \in G$. Then $\{I, t_0\}$ is normalized by the group $H = \left(\begin{smallmatrix} \mathbb{F}_q^\times & \\ & 1 \end{smallmatrix}\right)$ or by a dihedral group $D = H \rtimes \langle \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right) \rangle$ (Proposition 4.7). Suppose it is the former. We are going to count elements in $G \smallsetminus H$ of order 2 in two different ways to obtain a contradiction. Letting G act on the conjugacy class of t_0 by conjugation, the orbit-stabilizer theorem shows that there are $|G|/|H| = q(1+fq)$ elements conjugate to t_0, all of which have order 2. We note that the elements conjugate to t_0 in $N = \left(\begin{smallmatrix} 1 & \mathbb{F}_q \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mathbb{F}_q^\times & \\ & 1 \end{smallmatrix}\right)$ must fix ∞ and one other $\mathbb{F}_q$-rational point, so that there are q of them in N. Hence

$$\left|\left\{s \in G \smallsetminus N : s^2 = I\right\}\right| \geq q(1+fq) - q = fq^2.$$

An element of $s_i N$ is of the form

$$s_i t_{\lambda,\mu} = \begin{pmatrix} \alpha_i\lambda & \alpha_i\mu + \beta_i \\ \gamma_i\lambda & \gamma_i\mu + \delta_i \end{pmatrix},$$

and it has order 2 if and only if $\alpha_i\lambda + \gamma_i\mu + \delta_i = 0$. So given s_i and λ, there is at most one $\mu \in \mathbb{F}_q$ such that $s_i t_{\lambda,\mu}$ has order 2. Combining with the above lower bound for the number of elements of order 2, we have that

$$fq^2 \leq \left|\left\{s \in G \smallsetminus N : s^2 = I\right\}\right| \leq fq(q-1),$$

which is absurd. We conclude that t_0 is normalized by the dihedral group $D = \left(\begin{smallmatrix} \mathbb{F}_q^\times & \\ & 1 \end{smallmatrix}\right) \rtimes \left\langle \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right) \right\rangle$.

Applying the argument in the last paragraph to D instead of H, we find that the number of elements in $G \smallsetminus D$ conjugate to t_0 is precisely $\frac{1}{2}q(1+fq) - q = \frac{1}{2}q(fq-1)$. Since this is an integer, we conclude f must be odd. Moreover, it gives the lower bound

$$\left|\left\{s \in G \smallsetminus N : s^2 = I\right\}\right| \geq \frac{1}{2}q(fq-1). \tag{6.6}$$

We are going to count the number of elements of order 2 in $G \smallsetminus N$ in yet another way in order to bound f.

Since $\gamma_i \neq 0$ for any $i = 1, \ldots, fq$, we may assume that $\gamma_i = 1$ in what follows. Let n be the number of cosets $s_i N$ containing at least two elements of order 2. For each of these cosets, we may assume that s_i has order 2, so that $\delta_i = -\alpha_i$. Moreover, for each such i, there exists $(\lambda, \mu) \in \mathbb{F}_q^\times \times \mathbb{F}_q \smallsetminus \{(1,0)\}$ such that $s_i t_{\lambda,\mu}$ has order 2 — i.e.,

$$\mathrm{Tr}(s_i t_{\lambda,\mu}) = \alpha_i(\lambda - 1) + \mu = 0.$$

Hence $\alpha_i = \mu/(1-\lambda) \in \mathbb{F}_q$. For different choices of i, we get different values of $\alpha_i = s_i.\infty$ (Lemma 6.4), so that $n \leq |\mathbb{F}_q| = q$. Since $\alpha_i \in \mathbb{F}_q$, for fixed i and $\lambda \in \mathbb{F}_q^\times$, there exists a unique solution $\mu \in \mathbb{F}_q$ to the above trace equation. Hence there are precisely $q-1$ elements of order 2 in the coset $s_i N$, provided this coset has at least two elements of order 2.

Let m be the number of cosets $s_i N$ containing exactly one element of order 2. Note that $m + n \leq fq$, the total number of nontrivial cosets. The lower bound (6.6) for the number of elements of order 2 combined with the arguments in the last paragraph gives

$$\begin{aligned} \frac{1}{2}q(fq-1) \leq m + n(q-1) = m + n + n(q-2) \leq fq + q(q-2) \\ \implies f \leq \frac{2q-3}{q-2} = 2 + \frac{1}{q-2}. \end{aligned} \tag{6.7}$$

Since f is odd, we find $f = 1$, or $f = 3$ and $q = 3$.

6.2.1. *The case $f = 1$.* Here we have $|G| = |\Lambda|(1 + fq)q = q(q^2 - 1) = |\operatorname{PGL}_2(\mathbb{F}_q)|$. We now prove that $G \subset \operatorname{PGL}_2(\mathbb{F}_q)$, so that this containment must actually be equality.

We showed above that G contains an element of the form $\left(\begin{smallmatrix} 1 & \tau \\ & 1 \end{smallmatrix}\right)$ with $\tau \in k^\times$. For each $\mu \in \mathbb{F}_q$, we have

$$v_\mu := \begin{pmatrix} 1 & \mu \\ & 1 \end{pmatrix} \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} \begin{pmatrix} 1 & -\mu \\ & 1 \end{pmatrix} = \begin{pmatrix} \mu & \tau - \mu^2 \\ 1 & -\mu \end{pmatrix}.$$

As μ varies over the elements of $\mathbb{F}_q$, we get q distinct elements v_μ of order 2 satisfying $v_\mu.\infty = \mu$. Since none of them lies in N, each v_μ must lie in a distinct nontrivial coset $s_i N$ (Lemma 6.4). There are only $fq = q$ such cosets, so we conclude that every coset contains an element of order 2.

We have now shown that $N \subset \operatorname{PGL}_2(\mathbb{F}_q)$, and that each nontrivial coset representative may be chosen to have the form $s_i = \left(\begin{smallmatrix} \alpha_i & \beta_i \\ 1 & -\alpha_i \end{smallmatrix}\right)$ with $\alpha_i \in \mathbb{F}_q$. The final paragraph of §6.1.2 applies verbatim to show that $\beta_i \in \mathbb{F}_q$ as well, which proves that $G \subset \operatorname{PGL}_2(\mathbb{F}_q)$ as desired.

6.2.2. *The case $f = 3, q = 3$.* Here we find that $|G| = |\Lambda|(1 + fq)q = 60$. Note that all of the inequalities in (6.7) becomes equalities in this case, so that $n = 3$ and $m = 6$, and G contains $12+3 = 15$ elements of order 2. We showed at the beginning of this subsection that t_0 is normalized by a dihedral group D of order 4. Each such dihedral group D contains three of the elements of order 2, so that G contains five conjugate Klein 4-groups. Moreover, at the beginning of §6 we showed that the number of Sylow 3-subgroups is $1 + fq = 10$. It follows that G is icosahedral (Lemma 4.20).

7. Separably Closed Fields

Convention. Throughout this section we will assume that k is a separably closed field.

The goal of this section is to prove Theorem C and Theorem B *in the case were k is a separably closed field.* In this setting, Theorem B becomes:

Theorem 7.1. *Let k be a separably closed field of characteristic $p > 0$.*

1. *Fix q a power of p. There is exactly one conjugacy class of subgroups isomorphic to each of $\operatorname{PSL}_2(\mathbb{F}_q)$ and $\operatorname{PGL}_2(\mathbb{F}_q)$.*
2. *Let $n \in \mathbb{N} \smallsetminus p\mathbb{N}$. For each $m \in \mathbb{N}$ with $p^m n > 2$, the conjugacy classes of p-semi-elementary subgroups of order $p^m n$ are parameterized by the set of homothety classes of rank-m subgroups Γ with $\mu_n(k) \subset \Gamma \subset k$ via the map*
$$\Gamma \mapsto \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix}.$$
3. *Suppose that $p = 2$ and n is an odd positive integer. Let $\mathfrak{Dih}_n(k)$ denote the set of conjugacy classes of dihedral subgroups of $\operatorname{PGL}_2(k)$ of order $2n$. The map $\mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ defined by $G \mapsto \overline{\det}(t)$ for any involution $t \in G$ is well defined and bijective.*
4. *If $p = 3$, then there is exactly one conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.*

Any p-irregular subgroup of $\operatorname{PGL}_2(k)$ is among the four types listed here.

Remark 7.2. It is clear that this gives Theorem B when k is separably closed except perhaps when $p = 2$ and G is dihedral, in which case one must show that the quadratic form $x^2 + \lambda xy + y^2$ represents any nonzero element of k. Indeed, since k is separably closed, there exists a primitive n-th root of unity $\zeta \in k$, and hence the given quadratic form factors as $(x + \zeta y)(x + \zeta^{-1} y)$. For $\alpha \in k^\times$, we can see that this quadratic form represents α by simultaneously solving the linear equations $x + \zeta y = \alpha$ and $x + \zeta^{-1} y = 1$.

Tracing through the proofs in Sections 3–6, we find that there are only two ways in which the algebraically closed nature of k was used:

- To find a k-rational fixed point of $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, which was then conjugated to ∞. If $\gamma = 0$, then ∞ is a fixed point of s. So we may suppose $\gamma = 1$. Then the equation defining the fixed points of s is $z^2 + (\delta - \alpha)z - \beta = 0$. This polynomial is separable — in which case it will have a root in k — if and only if $p > 2$ or $p = 2$ and $\delta \neq \alpha$. So s fails to have a k-rational root if and only if $p = 2$, $\delta = \alpha$, and β is not a square in k. In particular, s must have order 2.
- To replace s with $\det(s)^{-1/2}s$ in order to assume $\det(s) = 1$. This was only used in §6.1, and scrutinizing its application shows that it can be dispensed with in the case q even. When q is odd, k contains all of its square roots.

This discussion shows that Theorem C holds for an arbitrary separably closed field, and Theorem 7.1 holds provided the characteristic of k is at least 3.

Convention. In the remainder of this section, we assume that k is a separably closed field of characteristic 2.

Let us summarize what we have learned.

Lemma 7.3. *Let $s \in \mathrm{PGL}_2(k)$ be an element with no k-rational fixed point. Then $s = \left(\begin{smallmatrix} \alpha & \beta \\ 1 & \alpha \end{smallmatrix}\right)$ for some $\alpha, \beta \in k$ with β a non-square. In particular, s has order 2.*

Lemma 7.4. *Let $G \subset \mathrm{PGL}_2(k)$ be a finite subgroup such that 4 divides the order of G. Then each Sylow 2-subgroup of G has a k-rational fixed point.*

Proof. Without loss of generality, we may replace G with any one of its Sylow 2-subgroups. Suppose that the proposition is false for G, and let $\rho \notin \mathbb{P}^1(k)$ be the unique fixed point of G. Over $k(\rho)$, we may conjugate G into the form $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ for some subgroup $\Gamma \subset k(\rho)$. More precisely, there exists $s = \left(\begin{smallmatrix} \alpha & \beta \\ 1 & \delta \end{smallmatrix}\right) \in \mathrm{PGL}_2(k(\rho))$ such that

$$s^{-1}Gs = \begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix}.$$

Note that the lower left entry of s is nonzero, else $G = s\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)s^{-1}$ fixes ∞.

Evidently $s.\infty = \rho$, which implies $\alpha = \rho$. For $\gamma \in \Gamma \smallsetminus \{0\}$, we have

$$s\begin{pmatrix} 1 & \gamma \\ & 1 \end{pmatrix}s^{-1} = \begin{pmatrix} \rho & \beta \\ 1 & \delta \end{pmatrix}\begin{pmatrix} 1 & \gamma \\ & 1 \end{pmatrix}\begin{pmatrix} \delta & \beta \\ 1 & \rho \end{pmatrix} = \begin{pmatrix} \beta/\gamma + (1+\delta/\gamma)\rho & \rho^2 \\ 1 & \beta/\gamma + (1+\delta/\gamma)\rho \end{pmatrix}.$$

Since $s\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)s^{-1} \subset \mathrm{PGL}_2(k)$, it follows that $1 + \delta/\gamma = 0$. But this uniquely determines the value of Γ, which is impossible since $|\Gamma| > 2$. This contradiction completes the proof. □

Let k_a be an algebraic closure of k. Theorem B applied to $\mathrm{PGL}_2(k_\mathrm{a})$ (which we proved in §6) shows that the finite p-irregular subgroups of $\mathrm{PGL}_2(k)$ are dihedral, p-semi-elementary, or isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ for some q. Each of the next three propositions covers one of these cases.

Proposition 7.5. *Fix an odd natural number n. Let $\mathfrak{Dih}_n(k)$ denote the set of k-conjugacy classes of dihedral subgroups of $\mathrm{PGL}_2(k)$ of order $2n$. Then the map $k^\times \to \mathfrak{Dih}_n(k)$ given by $\tau \mapsto G_\tau := \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right) \rtimes \left\{I, \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)\right\}$ induces a bijection*

$$k^\times/(k^\times)^2 \xrightarrow{\sim} \mathfrak{Dih}_n(k).$$

The inverse is given by $G \mapsto \overline{\det}(t)$ for any involution $t \in G$.

Proof. Recall that we are assuming k is separably closed of characteristic 2. Let G be a dihedral subgroup of $\mathrm{PGL}_2(k)$ of order $2n$, and let $\zeta \in k$ be a primitive n-th root of unity. We begin by showing that there is $\tau \in k^\times$ such that G is conjugate to

$$G_\tau = \left\langle \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix}, \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} \right\rangle.$$

If $|G| = 2$, choose any orbit of length 2 for the nontrivial element t of G and conjugate it to $\{0, \infty\}$. Any element of order 2 that stabilizes $\{0, \infty\}$ is of the form $\left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$ for some $\tau \in k^\times$, as desired.

If instead $|G| > 2$, then write $G = C \rtimes \langle t \rangle$ with C the index 2 cyclic normal subgroup of G and t an element of order 2. Since C has odd order, the quadratic polynomial defining its fixed points must have distinct — and hence k-rational — roots. Let us conjugate them to 0 and ∞ to get a new group $G' = \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right) \rtimes \langle t' \rangle$. Then t' acts on the fixed points of $\left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$, but it cannot fix both of them. Hence $t' = \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$ for some $\tau \in k^\times$.

It follows that the map $\tau \mapsto G_\tau$ has image equal to $\mathfrak{Dih}_n(k)$. Next we show that G_τ and $G_{\tau'}$ lie in the same conjugacy class if and only if $\tau' = \mu^2\tau$ for some $\mu \in k^\times$. One direction is easy: $\left(\begin{smallmatrix} \mu & \\ & 1 \end{smallmatrix}\right) G_\tau \left(\begin{smallmatrix} \mu^{-1} & \\ & 1 \end{smallmatrix}\right) = G_{\mu^2\tau}$. For the other direction, suppose that $s^{-1} G_\tau s = G_{\tau'}$ for some $s \in \mathrm{PGL}_2(k)$. If $|G| = 2$, set $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Then

$$\begin{pmatrix} & \tau' \\ 1 & \end{pmatrix} = s^{-1} \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} s = \begin{pmatrix} \alpha\beta + \gamma\delta\tau & \beta^2 + \delta^2\tau \\ \alpha^2 + \gamma^2\tau & \alpha\beta + \gamma\delta\tau \end{pmatrix}.$$

It follows that

$$\alpha\beta + \gamma\delta\tau = 0, \qquad \tau' = \frac{\beta^2 + \delta^2\tau}{\alpha^2 + \gamma^2\tau}.$$

If $\gamma\delta = 0$, then $\alpha\beta = 0$, and it follows that

$$\tau' = \left(\frac{\delta}{\alpha}\right)^2 \tau \quad \text{or} \quad \tau' = \left(\frac{\beta}{\gamma\tau}\right)^2 \tau.$$

If instead $\gamma\delta \neq 0$, then $\tau = \alpha\beta/\gamma\delta$, which implies that

$$\tau' = \frac{\beta^2 + \delta^2\tau}{\alpha^2 + \gamma^2\tau} = \frac{\beta\delta}{\alpha\gamma} = \left(\frac{\delta}{\alpha}\right)^2 \tau.$$

If $|G| > 2$, then s conjugates the index 2 normal subgroup of $G_{\tau'}$ to that of G_τ, which is to say that it lies in the normalizer of $\left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$. Hence $s = \left(\begin{smallmatrix} \mu & \\ & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} & \mu \\ 1 & \end{smallmatrix}\right)$ for some $\mu \in k^\times$. In these two cases, we have

$$s^{-1} \begin{pmatrix} & \tau \\ 1 & \end{pmatrix} s = \begin{pmatrix} & \mu^{-2}\tau \\ 1 & \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} & \mu^2\tau^{-1} \\ 1 & \end{pmatrix}.$$

Since these elements have order 2 in $G_{\tau'}$, there must be $\zeta \in \mu_n(k)$ such that

$$\begin{pmatrix} & \tau' \\ 1 & \end{pmatrix} = \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} \begin{pmatrix} & \mu^{-2}\tau \\ 1 & \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix} \begin{pmatrix} & \mu^2\tau^{-1} \\ 1 & \end{pmatrix}.$$

As the squaring map on $\mu_n(k)$ is surjective, it follows that ζ is a square in k, and hence τ' is equal to a square times τ, as desired.

Finally, observe that the determinant homomorphism $\overline{\det}$ is constant on conjugacy classes of $\mathrm{PGL}_2(k)$. Since every element of $\mu_n(k)$ is a square in k, the map $G_\tau \mapsto \overline{\det}(t)$ is well defined, where t is any involution in G_τ. Taking $t = \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$ shows that $G \mapsto \overline{\det}(t)$ is indeed the inverse to $\tau \mapsto G_\tau$. □

Lemma 7.6. *Let G be a finite subgroup of $\mathrm{PGL}_2(k)$ of even order. Define $k(G)/k$ to be the field extension generated by the fixed points of all Sylow 2-subgroups of G. (We define $k(\infty) = k$.) Then $k(G)/k$ has degree at most 2. If $[k(G) : k] = 2$, then every Sylow 2-subgroup of G is its own normalizer.*

Proof. Let P be a Sylow 2-subgroup of G. Recall that P is abelian and has a single fixed point in $\mathbb{P}^1(k_\mathrm{a})$, say ρ (Lemma 4.3). Since all Sylow 2-subgroups are conjugate, we have $k(G) = k(\rho)$. If $\rho \in \mathbb{P}^1(k)$, then $k(G) = k$. Otherwise, P does not have a k-rational fixed point. Let $s = \left(\begin{smallmatrix} \alpha & \beta \\ 1 & \alpha \end{smallmatrix}\right)$ be a nontrivial element of P (Lemma 7.3). Then the fixed point of s is given by the equation $z^2 = \beta \notin (k^\times)^2$, so that $\rho = \sqrt{\beta}$. Therefore $k(G)/k$ has degree 2.

Suppose now that u is an element of the normalizer of P, so that $u^{-1}Pu = P$. It follows that ρ is a fixed point of u. Since the fixed points of u are defined by an equation with k-coefficients, and since ρ is quadratic inseparable, it follows that ρ is the unique fixed point of u. Thus u has order 2 by Lemma 7.3, and $u \in P$. □

Proposition 7.7. *Suppose that $G \subset \mathrm{PGL}_2(k)$ is a finite 2-semi-elementary subgroup of order $2^m n > 2$, where n is odd. Then G is conjugate to a subgroup of the form*

$$\begin{pmatrix} 1 & \Gamma \\ & 1 \end{pmatrix} \rtimes \begin{pmatrix} \mu_n(k) & \\ & 1 \end{pmatrix},$$

where Γ is uniquely determined up to homothety in k.

Remark 7.8. The group corresponding to the excluded case $m = n = 1$ is dihedral, and hence falls under the purview of Proposition 7.5.

Proof. If we can show that G has a k-rational fixed point, then the arguments in Section 4.4 immediately imply that G is conjugate to a group of the desired form.

If $m > 1$, then Lemma 7.4 asserts the existence of a k-rational fixed point. Suppose now that $n > 1$. Over k_a, we may conjugate G to a group of the form $G' = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$, where $\Gamma \subset k_\mathrm{a}$ is a nontrivial additive subgroup. It follows that the Sylow 2-subgroup $P' = \left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right)$ has normalizer $N_{G'}(P') = G' \supsetneq P'$, and so the Sylow 2-subgroup of G also has nontrivial normalizer. Hence $k(G) = k$ by Lemma 7.6. That is, G has a k-rational fixed point. □

Finally, we treat subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{PSL}_2(\mathbb{F}_q)$. Note that when $q = 2$, this group is dihedral and hence has already been dealt with.

Proposition 7.9. *Let $q = 2^r$ for some $r > 1$. If $G \subset \mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, then it is k-conjugate to $\mathrm{PGL}_2(\mathbb{F}_q)$.*

Proof. Let P be a Sylow 2-subgroup of G. Then $|P| \geq 4$, and hence the fixed point of P must be k-rational (Lemma 7.4). The proof in §6 now proceeds *mutatis mutandis* to show that G is conjugate to $\mathrm{PGL}_2(k)$. □

8. Galois Descent

Convention. For this section, k denotes an arbitrary field of positive characteristic p, k_s denotes a separable closure of k, and $\mathfrak{g} = \mathrm{Gal}(k_\mathrm{s}/k)$.

We use the technique of Galois descent to pass from the classification of finite subgroups of PGL_2 over separably closed fields to the case of arbitrary fields. It begins with a result of Beauville:

Theorem 8.1 ([1, §2])**.** *Let G be an algebraic group defined over a field k, let H be a subgroup of $G(k)$, let $N = N_{G(k)}(H)$ be its normalizer in $G(k)$, and let Z be the centralizer of H in $G(k_\mathrm{s})$.*

Write $\mathrm{Conj}(H, G(k))$ *for the set of subgroups of* $G(k)$ *that are conjugate to* H *in* $G(k_\mathrm{s})$ *modulo conjugacy in* $G(k)$*. Then there is a canonical isomorphism of pointed sets*

$$\ker\Big[H^1(\mathfrak{g}, Z) \to H^1\big(\mathfrak{g}, G(k_\mathrm{s})\big)\Big] \;/\; N \xrightarrow{\sim} \mathrm{Conj}(H, G(k)).$$

Theorem 8.2. *Let* $H \subset \mathrm{PGL}_2(k)$ *be a finite* p*-irregular subgroup, and let* Z *be the centralizer of* H *in* $\mathrm{PGL}_2(k_\mathrm{s})$*.*

(1) *If* $|H| > 2$*, then* $H^1(\mathfrak{g}, Z) = 1$*.*
(2) *If* $|H| = p = 2$*, then there is a canonical isomorphism* $k/f(k,k) \xrightarrow{\sim} H^1(\mathfrak{g}, Z)$*, where* $f(x,y) = x^2 + y + \tau y^2$ *and* $\tau = \overline{\det}(t)$ *for the nontrivial element* $t \in H$*.*

In either case, the canonical homomorphism $H^1(\mathfrak{g}, Z) \to H^1(\mathfrak{g}, \mathrm{PGL}_2)$ *has trivial kernel.*

Applying Theorem 8.1, we find that $\mathrm{Conj}\,(H, \mathrm{PGL}_2(k))$ contains a unique element for any finite p-irregular subgroup H. We state this formally:

Corollary 8.3. *Let* H *be a finite* p*-irregular subgroup of* $\mathrm{PGL}_2(k)$*. If* $H' \subset \mathrm{PGL}_2(k)$ *is another subgroup that is conjugate to* H *inside* $\mathrm{PGL}_2(k_\mathrm{s})$*, then it is already conjugate inside* $\mathrm{PGL}_2(k)$*.*

Proof of Theorem 8.2. If H is contained in $\mathrm{PGL}_2(k)$, then evidently it is conjugate over k_s to one of the groups described in Theorem 7.1. Any element $s \in Z$ must stabilize the unique fixed point of any Sylow p-subgroup of H. If H is not dihedral of order 2 (with $p = 2$) or a p-semi-elementary subgroup, then H has at least 3 Sylow p-subgroups, and hence s fixes at least 3 points of $\mathbb{P}^1(k_\mathrm{s})$. That is $Z = 1$, and hence $H^1(\mathfrak{g}, Z) = 1$ for trivial reasons.

Next, suppose that H is a p-semi-elementary subgroup of $\mathrm{PGL}_2(k)$ of order $2^m n > 2$ with normal Sylow p-subgroup P. Then P fixes a unique point of k_a; we claim that the fixed point of P is actually k-rational. The defining equation for the fixed point of P is quadratic, and hence separable if $p > 2$, and hence k-rational. If $p = 2$, then we appeal to the proof of Proposition 7.7 to see that its fixed point is k-rational. In either case, we may replace H with one of its conjugates in order to assume that the fixed point of P is ∞.

The centralizer of P is precisely $U(k_\mathrm{s}) = \left(\begin{smallmatrix} 1 & k_\mathrm{s} \\ & 1 \end{smallmatrix}\right)$, and hence $Z \subset U(k_\mathrm{s})$. If $n > 1$, then H contains an element t of order prime to p. Any $s \in Z$ must also stabilize the finite fixed point of t, so that $Z = 1$, and $H^1(\mathfrak{g}, Z) = 1$. If $n = 1$, then $Z = U(k_\mathrm{s}) \cong \mathbb{G}_a(k_\mathrm{s})$ as $\mathfrak{g}$-modules. It is well known that $H^1(\mathfrak{g}, \mathbb{G}_a) = 1$ [6, Ch. X.1].

Now suppose that $p = 2$ and that H is dihedral of order 2. Choose a k-rational orbit in $\mathbb{P}^1(k)$ of length 2 for H, and let us conjugate this orbit to $\{0, \infty\}$. So without loss of generality, we may suppose that H is generated by $t = \left(\begin{smallmatrix} & \tau \\ 1 & \end{smallmatrix}\right)$ for some $\tau \in k^\times$. The centralizer of t is given by

$$Z = \left\{ \begin{pmatrix} \alpha & \tau\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in k, \alpha^2 + \tau\beta^2 \neq 0 \right\}.$$

Consider the short exact sequence of $\mathfrak{g}$-module homomorphisms

$$1 \longrightarrow Z \xrightarrow{\phi} \mathbb{G}_a \times \mathbb{G}_a \xrightarrow{f} \mathbb{G}_a \longrightarrow 0,$$

where

$$\phi \begin{pmatrix} \alpha & \tau\beta \\ \beta & \alpha \end{pmatrix} = \left(\frac{\alpha\beta}{\alpha^2 + \tau\beta^2}, \frac{\beta^2}{\alpha^2 + \tau\beta^2} \right) \quad \text{and} \quad f(x,y) = x^2 + y + \tau y^2.$$

(To see that $\ker(f) \subset \mathrm{im}(\phi)$, take $\alpha = x/y$ and $\beta = 1$ when $y \neq 0$.) Passing to the long exact sequence on cohomology and using the fact that $H^1(\mathfrak{g}, \mathbb{G}_a \times \mathbb{G}_a) \cong H^1(\mathfrak{g}, \mathbb{G}_a) \times H^1(\mathfrak{g}, \mathbb{G}_a) = 1$, we see that

$$H^0(\mathfrak{g}, \mathbb{G}_a \times \mathbb{G}_a) \xrightarrow{f} H^0(\mathfrak{g}, \mathbb{G}_a) \xrightarrow{\delta} H^1(\mathfrak{g}, Z) \longrightarrow 1.$$

The coboundary map δ induces the desired isomorphism $k/f(k,k) \xrightarrow{\sim} H^1(\mathfrak{g}, Z)$.

Finally, we must show that kernel of the homomorphism $H^1(\mathfrak{g}, Z) \to H^1(\mathfrak{g}, \mathrm{PGL}_2)$ is trivial. It is obvious from our above work if $|H| > 2$, so let us assume that $|H| = p = 2$. Keeping with the above notation, if $\sqrt{\tau} \in k$, then $f(k, k) = k$. Indeed, for any $\gamma \in k$, we have $f(\gamma\sqrt{\tau}, \gamma) = \gamma$. Hence $H^1(\mathfrak{g}, Z) = 1$, and again the kernel is obviously trivial.

Now we assume that $|H| = p = 2$ and $\sqrt{\tau} \notin k$. Let $z_s : \mathfrak{g} \to Z$ be a 1-cocycle that becomes a coboundary when its target is extended to PGL_2. Then there exists $u \in \mathrm{PGL}_2(k_\mathrm{s})$ such that $z_s = u^{-1}({}^s u)$ for every $s \in \mathfrak{g}$. Since every element of Z fixes $\sqrt{\tau}$, we see that

$$\sqrt{\tau} = z_s.\sqrt{\tau} = u^{-1}({}^s u).\sqrt{\tau} \;\Rightarrow\; u.\sqrt{\tau} =^s u.\sqrt{\tau} =^s (u.\sqrt{\tau}).$$

The final equality follows from the fact that $\sqrt{\tau}$ lies in a purely inseparable extension of k, so that $\mathfrak{g}$ acts trivially on it. Thus $u.\sqrt{\tau}$ is defined over $k(\sqrt{\tau})$. Note that $u.\sqrt{\tau} \notin \mathbb{P}^1(k)$ since that would imply $\sqrt{\tau} = u^{-1}.(u.\sqrt{\tau}) \in \mathbb{P}^1(k_\mathrm{s})$. Choose $v \in \mathrm{PGL}_2(k)$ such that $v.(u.\sqrt{\tau}) = \sqrt{\tau}$. Then $vu \in Z$, and $z_s = (vu)^{-1} \cdot {}^s(vu)$. That is, z_s is already a coboundary, and hence trivial in $H^1(\mathfrak{g}, Z)$. □

We now prove Theorem A and the most general version of Theorem B simultaneously.

Proof of Theorems A and B. As $\mathrm{PGL}_2(k) \subset \mathrm{PGL}_2(k_\mathrm{s})$, the isomorphism type of a finite p-irregular subgroup of $\mathrm{PGL}_2(k)$ must be among those in Theorem 7.1.

We treat the case of p-semi-elementary subgroups first. Suppose that H is a p-semi-elementary subgroup of $\mathrm{PGL}_2(k)$ with $|H| > 2$. The fixed point of the Sylow p-subgroup of H is k-rational: if $p > 2$, it is the unique root of a quadratic polynomial, and if $p = 2$ we apply Proposition 7.7. The technique in §4.4 shows that H is conjugate to a subgroup of the form $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$ for some subgroup $\Gamma \subset k$ of order p^m and some integer n coprime to p, with $\mu_n(k_\mathrm{s}) = \mu_n(k) \subset \Gamma$. This immediately implies $\dim_{\mathbb{F}_p}(k) \geq \dim_{\mathbb{F}_p}(\Gamma) = m$. Letting e be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, Remark 4.9 shows that Γ is an $\mathbb{F}_{p^e}$-vector space, which implies that $e \mid m$. The pair (Γ, n) uniquely determines the $\mathrm{PGL}_2(k_\mathrm{s})$-conjugacy class of H up to homothety of Γ in k_s (Theorem 7.1); the preceding corollary allows us to replace k_s with k in this last statement.

To complete the proof of Theorem A for p-semi-elementary subgroups, suppose that $n \in \mathbb{N} \smallsetminus p\mathbb{N}$ is such that k contains a primitive n-th root of unity, that $m \in \mathbb{N}$, that e is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, and the $e \mid m \leq \dim_{\mathbb{F}_p}(k)$. Let Γ be any $\mathbb{F}_{p^e}$-subspace of k of rank m/e and observe that $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_n(k) & \\ & 1 \end{smallmatrix}\right)$ is a p-semi-elementary subgroup of $\mathrm{PGL}_2(k)$ of the desired order.

Now we turn to subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$. Theorem 7.1 shows there is a unique $\mathrm{PGL}_2(k_\mathrm{s})$-conjugacy class of subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q)$, and the preceding corollary implies there is at most one conjugacy class in $\mathrm{PGL}_2(k)$. Evidently it is sufficient that k contain $\mathbb{F}_q$ for these subgroups to exist. For the necessity statement, suppose that $H \subset \mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, and let $H' \subset H$ be a Borel subgroup. Then H' is a p-semi-elementary group, and the preceding paragraph shows that H' is conjugate in $\mathrm{PGL}_2(k)$ to one of the form $\left(\begin{smallmatrix} 1 & \Gamma \\ & 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mathbb{F}_q^\times & \\ & 1 \end{smallmatrix}\right)$ with $\mathbb{F}_q^\times \subset \Gamma \subset k$. It follows that $\mathbb{F}_q \subset k$. If instead we start with a subgroup H that is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$, then the same argument shows that $(\mathbb{F}_q^\times)^2 \subset k$. But the set of nonzero squares in $\mathbb{F}_q$ generates the field extension $\mathbb{F}_q/\mathbb{F}_p$, so that $\mathbb{F}_q \subset k$.

Next we assume $p = 2$ and deal with existence of dihedral subgroups of order $2n$ (n odd). If $n = 1$, then $\mathrm{PGL}_2(k)$ always contains the dihedral subgroup $\{I, \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)\}$, and $\lambda = \zeta + \zeta^{-1} = 0 \in k$. Next suppose that $n > 1$. If ζ is a primitive n-th root of unity such that $\lambda = \zeta + \zeta^{-1} \in k$, then we set $s = \left(\begin{smallmatrix} \lambda+1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ and $t = \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$. The corollary to Proposition 4.1 shows that s has order n, and direct calculation shows that $tst = s^{-1}$. That is, $\langle s, t\rangle \subset \mathrm{PGL}_2(k)$ is dihedral. Conversely, suppose that $H \subset \mathrm{PGL}_2(k)$ is any dihedral group of order $2n$. In particular, H contains a 2-regular cyclic subgroup of order n, which shows that $\zeta + \zeta^{-1} \in k$ for some primitive n-th root of unity ζ [1,

Prop. 1.1]. This proves Theorem A for dihedral groups, and it remains to prove Theorem B in this case.

Suppose that $p = 2$, that $\lambda = \zeta + \zeta^{-1} \in k$ for some primitive n-th root of unity (n odd), and that $G \subset \mathrm{PGL}_2(k)$ is dihedral of order $2n$. If $n = 1$, then the argument and conclusion of Proposition 7.5 applies verbatim. So let us suppose that $n > 1$. We show that G is conjugate to the subgroup

$$G_{\alpha,\beta} = \left\langle \begin{pmatrix} \lambda+1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \alpha\lambda+\beta \\ \beta & \alpha \end{pmatrix} \right\rangle.$$

Since n is odd, there is a unique conjugacy class of cyclic subgroups of order n in $\mathrm{PGL}_2(k)$ [1, Thm. 4.2]. The element $s = \left(\begin{smallmatrix} \lambda+1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ generates a subgroup of order n (Corollary to Proposition 4.1), so after an appropriate conjugation we may assume that G contains s. Now G is generated by s and an element of order 2, say $t = \left(\begin{smallmatrix} \alpha & \beta' \\ \beta & \alpha \end{smallmatrix}\right)$, such that $tst = s^{-1}$. A direct computation shows that this relation holds if and only if $\beta' = \alpha\lambda + \beta$, as desired. Every involution in G is of the form $s^i t$ for some $i = 0, \ldots, n-1$, and we see immediately that

$$\overline{\det}(s^i t) = \lambda^i(\alpha^2 + \lambda\alpha\beta + \beta^2) = \alpha^2 + \lambda\alpha\beta + \beta^2 \mod (k^\times)^2.$$

Hence the map $\mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ defined by $G \mapsto \overline{\det}(t)$ for any involution $t \in G$ is well defined with image equal to the set of nonzero elements of k represented by the quadratic form $x^2+\lambda xy+y^2$. To see that $\mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ is injective, consider the commutative diagram

$$\begin{array}{ccc} \mathfrak{Dih}_n(k) & \longrightarrow & \mathfrak{Dih}_n(k_\mathrm{s}) \\ \downarrow & & \downarrow \\ k^\times/(k^\times)^2 & \longrightarrow & k_\mathrm{s}^\times/(k_\mathrm{s}^\times)^2 \end{array}$$

The vertical arrows are the maps induced by the determinant. The upper horizontal arrow is the natural map from k-conjugacy classes to k_s-conjugacy classes, which is injective by Corollary 8.3. The lower horizontal arrow is the canonical inclusion. The right vertical map is an isomorphism by Proposition 7.5. Hence the left vertical map is also an injection.

Finally, suppose that $p = 3$. If $G \subset \mathrm{PGL}_2(k)$ is an icosahedral subgroup, then it contains a subgroup of order 5. By [1, Prop. 1.1], we see that $\lambda := \zeta + \zeta^{-1} \in k$ for some primitive fifth root of unity ζ. But λ is quadratic over $\mathbb{F}_3$, with minimal polynomial $X^2 + X - 1$, and hence it generates $\mathbb{F}_9$. That is, $\mathbb{F}_9 \subset k$. Conversely, if we assume that $\mathbb{F}_9 \subset k$, then define

$$s = \begin{pmatrix} \lambda+1 & -1 \\ 1 & 1 \end{pmatrix} \qquad t = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}.$$

Then a direct calculation shows that s has order 5, that $t^2 = I$, and that st has order 3. It follows that the subgroup $\langle s, t \rangle \subset \mathrm{PGL}_2(\mathbb{F}_9)$ is isomorphic to $\mathfrak{A}_5$ (Lemma 4.21). As above, Theorem 7.1 and Corollary 8.3 show that there is at most one conjugacy class of icosahedral subgroups in $\mathrm{PGL}_2(k)$. □

Proof of Theorem D. Let us first consider the p-regular subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$. Theorem C gives the list of possible isomorphism types of subgroups for us to consider. Conditions for existence and a classification of conjugacy classes are given by [1, Prop. 1.1, 4.2]; we will use these two results without further comment.

We begin with cyclic subgroups of order n. If $n \mid (q-1)$, and if $\zeta \in \mathbb{F}_q^\times$ is a generator, then $\left(\begin{smallmatrix} \zeta^{(q-1)/n} & \\ & 1 \end{smallmatrix}\right)$ evidently generates a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ of order n. If instead $n \mid (q+1)$, and if we take $\xi \in \mathbb{F}_{q^2}^\times$ to be a generator, then $\varepsilon = \xi^{(q^2-1)/n}$ is an element of order n with the property that $\varepsilon^q = \varepsilon^{-1}$. In particular, $\lambda = \varepsilon + \varepsilon^{-1} \in \mathbb{F}_q$, and so $\left(\begin{smallmatrix} \lambda+1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ generates a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$

of order n (Corollary 4.2). A dihedral subgroup of order $2n$ may be generated by $\left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$ along with either of the previous two matrices.

Conversely, suppose $s \in \mathrm{PGL}_2(\mathbb{F}_q)$ generates a cyclic subgroup of order n (prime to p). Then s has two distinct fixed points in $\overline{\mathbb{F}}_q$. If these fixed points are $\mathbb{F}_q$-rational, then without loss of generality we may conjugate them to 0 and ∞ in order to assume that $s = \left(\begin{smallmatrix} \alpha & \\ & 1 \end{smallmatrix}\right)$ for some $\alpha \in \mathbb{F}_q^\times$ of order n. It follows that n divides $q-1$. If instead the fixed points of s are quadratic over $\mathbb{F}_q$, then we may write them as ε and ε^q for some $\varepsilon \in \mathbb{F}_{q^2}^\times \smallsetminus \mathbb{F}_q^\times$. Write $s = \left(\begin{smallmatrix} \alpha & \beta \\ 1 & \delta \end{smallmatrix}\right)$; note that the lower left entry is certainly nonzero, else ∞ is a fixed point of s. Set $u = \left(\begin{smallmatrix} 1 & -\varepsilon \\ 1 & -\varepsilon^q \end{smallmatrix}\right)$ and $\omega = (\alpha - \varepsilon)/(\alpha - \varepsilon^q)$. Using the fact that ε and ε^q satisfy $z^2 - (\alpha - \delta)z - \beta$, the defining polynomial for the fixed points of s, a direct calculation gives $usu^{-1} = \left(\begin{smallmatrix} \omega & \\ & 1 \end{smallmatrix}\right)$. We also see that $\omega^q = \omega^{-1}$, and hence $\omega^{q+1} = 1$. That is, s has order dividing $q+1$ as desired. Hence a cyclic subgroup of order n (and also a dihedral group of order $2n$) exists if and only if $q \equiv \pm 1 \pmod{n}$. There is a unique conjugacy class of such subgroups.

For any prime p, it is a standard fact about the field $\mathbb{F}_p$ that the equation $x^2 + y^2 = -1$ has a solution. Hence for $p > 3$, there exist subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ isomorphic to $\mathfrak{A}_4$ (resp. $\mathfrak{S}_4$), and they all lie in a single conjugacy class. For $p > 5$, quadratic reciprocity shows that $\sqrt{5} \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod{5}$, and it lies in $\mathbb{F}_{p^2}$ when $p \equiv \pm 2 \pmod{5}$. So $\mathrm{PGL}_2(\mathbb{F}_q)$ contains a unique conjugacy class of icosahedral subgroups when $p \equiv \pm 1 \pmod{5}$ or when $p \equiv \pm 2 \pmod{5}$ and $r = [\mathbb{F}_q : \mathbb{F}_p]$ is even.

Now we treat the p-irregular subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ using Theorems A and B. It follows immediately that $\mathrm{PGL}_2(\mathbb{F}_q)$ contains subgroups isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{p^s})$ and $\mathrm{PSL}_2(\mathbb{F}_{p^s})$ if and only if $\mathbb{F}_{p^s} \subset \mathbb{F}_q$ if and only if $s \mid r$. There is only one conjugacy class of each type of subgroup. Observe that $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$ and $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$, which fits into the description of tetrahedral and octahedral subgroups in the statement of Theorem D. We may also deal with icosahedral groups in characteristic 2 by noting that $\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$; in this case $\mathrm{PGL}_2(\mathbb{F}_q)$ contains a unique class of icosahedral subgroups precisely when $r = [\mathbb{F}_q : \mathbb{F}_p]$ is even. In characteristic 5, we note that $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

Next consider the p-semi-elementary subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ of order $p^m n$ with $p \nmid n$. Let e be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. To have such a subgroup in $\mathrm{PGL}_2(\mathbb{F}_q)$, we must have $e \mid r$ and $e \mid m \leq r = \dim_{\mathbb{F}_p}(\mathbb{F}_q)$. Under these conditions, Theorem B guarantees that the p-semi-elementary subgroups are in one-to-one correspondence with homothety classes of rank-m subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ containing $\mathbb{F}_{p^e}$. Observe also that when $p = 2$, the group $\mathfrak{A}_4$ is 2-semi-elementary, and therefore such subgroups exist in $\mathrm{PGL}_2(\mathbb{F}_q)$ if and only if $\mathbb{F}_4 \subset \mathbb{F}_q$. In the latter case, it must be conjugate to $B(\mathbb{F}_4)$; in particular, the conjugacy class of tetrahedral subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ is unique when q is even.

There are two types of p-irregular dihedral subgroups of order $2n$ in $\mathrm{PGL}_2(\mathbb{F}_q)$, depending on whether or not p divides n. If $p \mid n$, then we must have $p = n$ since any p-irregular cyclic subgroup has order p. But such groups are p-semi-elementary and have already been treated. If instead $p \nmid n$, then $p = 2$. We know that such subgroups exist if and only if $\mathbb{F}_q$ contains $\zeta_n + \zeta_n^{-1}$ for some primitive n-th root of unity ζ_n, or that $n \mid q^2 - 1$. Moreover, the conjugacy classes are parameterized by a subgroup of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 = 1$; that is, there is only one conjugacy class.

Finally, we note that in characteristic 3 there is exactly one conjugacy class of icosahedral subgroups if and only if $\mathbb{F}_9 \subset \mathbb{F}_q$, or equivalently $r = [\mathbb{F}_q : \mathbb{F}_p]$ is even. □

References

[1] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[2] H. S. M. Coxeter. *Regular polytopes*. Dover Publications Inc., New York, third edition, 1973.

[3] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.
[4] Xander Faber, Michelle Manes, and Bianca Viray. Computing automorphism groups of rational functions. Preprint, arXiv:1202.5557v1 [math.NT], 2012.
[5] Felix Klein. *Lectures on the icosahedron and the solution of equations of the fifth degree*. Dover Publications Inc., New York, N.Y., revised edition, 1956. Translated into English by George Gavin Morrice.
[6] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.
[7] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
[8] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

Department of Mathematics, University of Hawai'i at Mānoa, Honolulu, HI
E-mail address: xander@math.hawaii.edu